รายงานวิจัย

การออกแบบและการพัฒนาระบบซึ่งมีความปลอดภัย กรณีระบบสลากกินแบ่งออนไลน์

Design and Implementation of a Secure System: A Case of Online Lottery System

ผู้ช่วยศาสตราจารย์ ดร.ปราโมทย์ กั่วเจริญ

เมษายน 2556

สถาบันบัณฑิตพัฒนบริหารศาสตร์

Final Report

Design and Implementation of a Secure System:

A Case of Online Lottery System

(การออกแบบและการพัฒนาระบบซึ่งมีความปลอดภัย กรณีระบบสลากกินแบ่งออนไลน์)

Assistant Professor Pramote Kuacharoen, Ph.D.

National Institute of Development Administration

Contents

Chapter 1 Introduction

1.1. Significance of the Research

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction [1]. The requirements of information security have undergone changes in the last several decades. When data was not accessible remotely, the security of information that was valuable was provided primarily by physical and administrative means. However, with the use of networks and communications facilities for carrying data between computers, different measures are needed to protect data. The importance of information security to the economic and national security interests has been recognized. The Federal Information Security Management Act (FISMA) defines three levels potential impact; namely, low, moderate, and high, on organizations and individuals should there be a breach of security [2]. For a system that has a high level of the potential impact, a breach of security could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. Therefore, such a system demands a high level of security requirements. Examples of high level potential impact systems are electronic voting systems, classified document systems, and lottery systems. In this research, a system with a high level of potential impact will be designed and implemented. The secure system will be applied to an online lottery system which has a significant implication in a high level of security requirements.

Government has the authority to operate lottery schemes. Since the government has total control of the operation of the lottery system, the integrity of such systems becomes questionable. Public trust cannot be achieved. The people may speculate that the lottery is rigged. This issue becomes critical with an online lottery system since the unprotected data can be easy manipulated. If all of the sold combinations are known before the drawing, the government may rig the lottery so that the winning numbers are the least played combinations. Moreover, winning tickets may be added after the drawing. As a result, corruption may be inevitable.

According to the United Nations, good governance consists of eight major characteristics, namely, participatory, consensus oriented, accountable, transparent, responsive, effective and efficient, equitable and inclusive, and following the rule of law [3]. The government should practice good governance through the operation the lottery system. The operation of the government should be transparent, open to scrutiny, and can be monitored by the people. This will reduce corruption in the government.

Furthermore, the operation of the lottery should adhere to the core values of the World Lottery Association which are responsibility, integrity, professionalism, and innovation [4]. The integrity value includes transparency and accountability. These are also important elements in good governance.

Besides promoting good governance, a secure online lottery system demonstrates the use of modern cryptography to provide security services which ensures adequate security of the systems. The security services can be divided into five categories, namely, authentication, access control, data

confidentiality, data integrity, and non-repudiation. Various services will be used in designing and implementing the system.

When changing from a paper-based lottery system to an online lottery system, different types of threats emerge. Threats from cybercrime become prevalent. An assault on system security may be in the form of active attack or passive attack [5]. An active attack attempts to alter resources or affect the operation whereas a passive attack tries to obtain information. Without proper preventions, a reliable service cannot be offered.

Finally, through the application of cryptography, this research can be used as a case study in teaching cryptography and network security. The research illustrates how to apply cryptographic knowledge to mitigate social science issues. It is an interdisciplinary research which involves two unrelated academic disciplines.

1.2. Purpose of the Research

The purpose of this research is to design and implement an online lottery system which is secure. The following properties are the design goals of the secure online lottery system.

- Accuracy: A system is accurate if it is not possible for the sold lottery numbers to be modified.
- Privacy: A system is private if neither authorities nor anyone else can reveal the identity of the buyer without the buyer's consent.
- Transparency: A system is transparent if it does not permit the authorities or anyone to obtain information from the system on the lottery numbers sold before the drawing and to add new numbers after the drawing.
- Verifiability: A system is verifiable if the buyer can claim the winning number even the data in the system is completely destroyed.

1.3. Scope of the Research

The research will encompass three main parts. The first part will be an understanding of requirements in a lottery system. The second part will be a design of a secure online lottery system using cryptographic methodology and network security. The third part will be an implementation of a secure online lottery system.

Chapter 2 An Overview of Information Security

2.1. The OSI Security Architecture

ITU-T Recommendation X.800 [7], Security Architecture for OSI, defines such a systematic approach. The OSI security architecture is useful to managers as a way of organizing the task of providing security. The OSI security architecture provides a general description of security attacks, security services, and related mechanisms. These can be defined briefly as follows:

- Security Attack: Any action that compromises the security of information owned by an organization.
- Security Service: A processing or communication service that provides a specific type of protection to system resources by implementing security policies using security mechanisms.
- Security Mechanism: A process that is designed to detect, prevent or recover from a security attack.

2.2. Security Attacks

A security attack is an assault on system security which can be classified in terms of passive attacks and active attacks. A passive attack attempts to learn or make use of information from the system by does not affect system resources. On the other hand, an active attack attempts to alter system resources or affect their operation.

Passive Attacks

Passive attacks are to observe or eavesdrop on transmissions with a goal to obtain information that is being transmitted. The attacker can learn the content of information or can analyze the traffic. For instance, the attacker eavesdrops an email message which is in transit to the mail server. The content of the email is revealed to the attacker. If the message is encrypted, the attacker cannot directly read the message. However, even if the information from the observed message cannot be extracted, the attacker can learn the identities, locations, or patterns of the communications.

Since passive attacks, if realized, would not result in any modification to any information contained in the system or affecting the normal operation, passive attacks are very difficult to detect. However, it can be easily prevented usually by means of encryption.

Active Attacks

Active attacks involve some alteration of the information or changes to the operation of the system. There are four categories of active attacks, namely, masquerade, replay, modification of messages, and denial of service.

- A masquerade is where one entity pretends to be another. A masquerade is usually used with some other forms of active attack, especially replay and modification of messages.

- A reply involves passively obtaining of a message or part of a message and repeating it to produce an unauthorized effect. For example, a valid message containing authentication information may be replayed by an attacker to gain access to the system.
- Modification of a message occurs when the content of a data transmission is altered without detection and results in an unauthorized consequence.
- Denial of service prevents the normal operation of the system. For example, an attacker causes the ecommerce site to stop responding to a valid transaction.

In comparison to passive attacks, active attacks can be easily detected. However, it is quite difficult to prevent active attacks completely. The goal is to detect active attacks and to recover from any disruption or delays cause by them.

2.3. Security Services

X.800 defines security services to ensure adequate security of the systems or of data transfers. These services are categorized into authentication, access control, data confidentiality, data integrity, and non-repudiation. These services can be applied to the data in storage as well. A brief description of each category is described below.

1. Authentication: The authentication service is concerned with assuring that a communication is authentic. It is the process of reliably verifying the identity of someone.
2. Access control: This service has the ability of limit or control the access to systems and applications via communication links. Unauthorized access is denied.
3. Data confidentiality: The confidentiality service protects transmitted data from passive attacks. This service also provides protection of data saved in storage.
4. Data integrity: This service ensures that data received are the same as sent by an authorized entity.
5. Non-repudiation: The non-repudiation service prevents either sender or receiver from denying a transmitted or produce message.

2.4. Security Mechanisms

X.800 defines specific security mechanisms and pervasive security mechanisms.

The specific security mechanisms may be incorporated into the appropriate layer in order to provide some of the services described earlier. The specific security mechanisms are described as follows.

1. Encipherment: The use of mathematical algorithms to transform data into an encrypted form. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys. Encipherment can provide confidentiality of either data or traffic flow information.
2. Digital Signature: Data appended to a data unit that allows the recipient of the data unit to prove the source and integrity of the data unit. This protects against forgery.
3. Access Control: These mechanisms may use the authenticated identity of an entity or information about the entity or capabilities of the entity, in order to determine and enforce the access rights of the entity.

4. Data Integrity: These mechanisms used to assure the integrity of a data unit or stream of data unit.
5. Authentication Exchange: This mechanism ensures the identity of an entity by means of information exchange.
6. Traffic Padding: A technique provides protection against traffic analysis by inserting bits into gaps in a data stream.
7. Routing Control: This enables the selection of particular physically secure routes for certain data to be transferred on.
8. Notarization: The mechanism uses a trusted third party to assure certain properties of data exchange.

Pervasive security mechanisms are not specific to any particular OSI security service or protocol layer. In general, the importance of these mechanisms is directly related to the level of security required.

1. Trusted Functionality: Any functionality which directly provides, or provides access to, security mechanisms, should be trustworthy.
2. Security Label: Resources may have security labels associated with them.
3. Event Detection: This allows the detection of certain security-relevant events which include the detection of apparent violations of security and normal events, such as a successful access.
4. Security Audit Trail: Data collected and potentially used to facilitate a security audit.
5. Security Recovery: This deals with request from mechanisms such as event handling and management functions, and takes recovery actions as the result of applying a set of rules.

2.5. Cryptography

Cryptography is one of the most important aspects of communications security. Modern cryptography is heavily based on mathematical theory and computer science practice; cryptography algorithms are designed around computational hardness assumptions, making such algorithms difficult to break in practice by attackers. The encryption algorithm is said to be computationally secure if the following criteria are met.

- The cost of breaking the cipher exceeds the value of the encrypted information.
- The time required to break the cipher exceeds the useful lifetime of the information.

Two forms of cryptography are symmetric and asymmetric [8], [9], [10].

Symmetric Cryptography

In symmetric cryptography, a single key is used in encryption and decryption. Symmetric cryptography is sometimes referred to as conventional cryptography or secret key cryptography. Figure 1 shows the processes for encryption and decryption. For encryption, the original message called plaintext is transformed using a secret key. The encryption is a cryptographic process that turns the plaintext into seemingly random bits called the ciphertext. Without the secret key, it would be extremely difficult to transform the ciphertext back to the plaintext. However, with the secret key, the ciphertext can be easily decrypted to obtain the original plaintext. It is impossible in practice to keep cipher, which is a specific mathematical process used in encryption and decryption,

secret. Usually, the cipher algorithm is well known and well tested. In order to provide confidentiality, the key must be kept secret. The most well-known symmetric cryptography algorithm is the Data Encryption Standard (DES) [11]. However, its strength is now questionable [12]. DES will be replaced by a more secure symmetric cryptography algorithm, the Advanced Encryption Standard (AES) [13]. The National Institute of Standards and Technology (NIST) released the AES in 2001. AES is efficient enough in terms of processing power and RAM requirements to be used on a wide variety of devices. AES offers three alternative key lengths: 128 bits, 192 bits, and 256 bits. Even the 128-key key length is strong. A brute force attack would take over 100 trillion years.

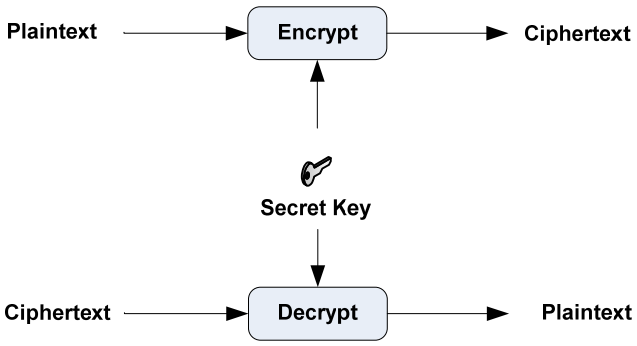

Figure 1. Encryption and Decryption for Symmetric Cryptography

Security uses of symmetric cryptography are transmitting over an insecure channel, secure storage on insecure media, and authentication. If two parties have agreed on a shared secret key, by using symmetric cryptography, one party can encrypt the message before sending over an insecure channel. The other party can then decrypt the message. If an attacker eavesdrops on the transmission, the attacker will only obtain unintelligible data. For secure storage, one can ensure that no one else can look at the stored information by encrypting it. If two parties share a secret key, one can send a random number which is known as a challenge for the other to encrypt. The encrypted random number called the response is sent back to the challenger. If the challenge can decrypt the response and obtain the same value as the challenge, the responder knows the shared key. Hence, the responder is authenticated.

Asymmetric Cryptography

In asymmetric cryptography or public key cryptography, on the other hand, two keys, namely, public key and private key are used. These two keys are mathematically related. Unlike symmetric cryptography, keys are not shared. A public key is preferably known to the entire world and a private key must not be revealed to anyone. Data encryption is performed by using the public key of the receiver of the message. The receiver can use the corresponding private key to decrypt the message. Figure 2 depicts the encryption and decryption process.

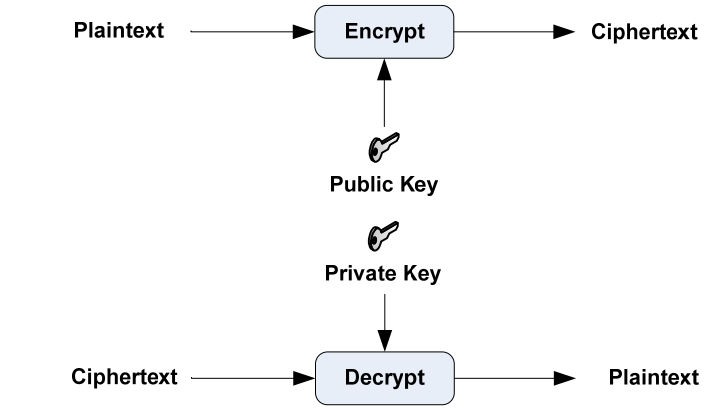

Figure 2. Encryption and Decryption for Asymmetric Cryptography

Asymmetric cryptography enables the generation of a digital signature. The digital signature is created from a message and the private key of the message composer. Therefore, a valid digital signature gives a recipient reason to believe that the message was created by a known sender. No one else can generate the digital signature, except the owner of the private key. As illustrated in Figure 3, a simplified signature generation is conducted using the plaintext and the private key to obtain a signed message and the simplified signature verification is done using the corresponding public key to obtain the original plaintext.

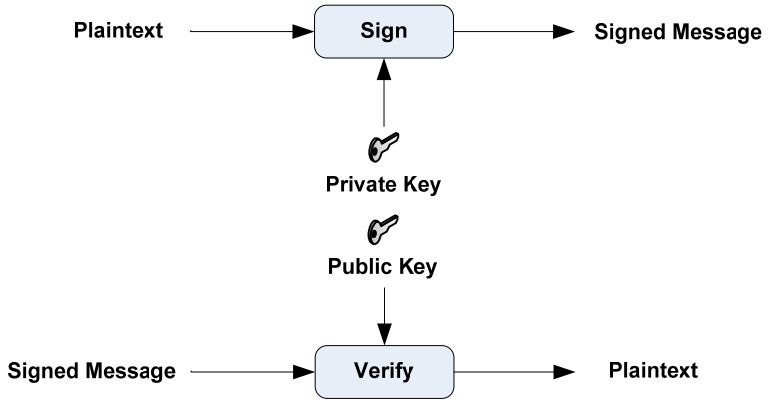

Figure 3. Signature Generation and Verification

The security uses of asymmetric cryptography include transmitting over an insecure channel, secure storage on insecure media, authentication and digital signatures. For transmitting over an insecure channel, the sender can use the recipient's public key to encrypt the message and then sends the encrypted message. Without the knowledge of the recipient's private key, the message cannot be decrypted. However, the recipient can easily decrypt the message. For secure storage, the owner of the information can use the public key to encrypt the information and stores on insecure media. The encrypted information can be easily decrypted using the corresponding private key. For authentication, the party can send a random number to the other as a challenge. The recipient encrypts the number using the private key and sends it back to the challenger as a response. The challenger can decrypt the response with the recipient's public key. If the two values are identical, the owner of the public key is authenticated. Finally, for the digital signatures, the message composer can sign the message using the private key. As mentioned earlier, the signature depends on both message and the private key. Anyone can verify that the message indeed was created by a

known author by using the author's public key. The most widely used asymmetric algorithm is RSA [14].

Cryptographic Hash Functions

A cryptographic hash function is an algorithm that takes a variable-length block of data as input and returns a fixed size bit string known as the hash value or the message digest. The cryptographic hash function has the following properties:

- Variable input size: H can be applied to an arbitrary block of data
- Fixed output size: H produces a fixed-length output
- Efficiency: It is easy to compute the hash value for any given message.
- Preimage resistant (one-way property): It is infeasible to generate a message that has a given hash. For any given hash value h, it is computationally infeasible to find y such that H(y) = h.
- Second preimage resistant (weak collision resistant): It is infeasible to modify a message without changing the hash. For any given block x, it is computationally infeasible to find y ≠ x with H(y) = H(x).
- Collision resistant (strong collision resistant): It is infeasible to find two different messages with the same hash. It is computationally infeasible to find any pair (x,y) such that H(x) = H(y).

The secure hash can be used to verify the message integrity. Determining whether any changes have been made to a message can be accomplished by comparing the message digest calculated before and after a transmission. For example, hash value can be used as message authentication. Figure 4 show a simplified example of the use of a hash function for message authentication with confidentiality. After the hash value is computed, both message and its hash value are encrypted using a secret key and are sent to the recipient. When the recipient receives the encrypted transaction, the message and the hash value can be obtained. The recipient can create the hash value and can compare the calculated hash value with the one received. If both values are equal, the message has not been modified. Since only the sender and the recipient share the secret key, the message must have been sent by the sender.

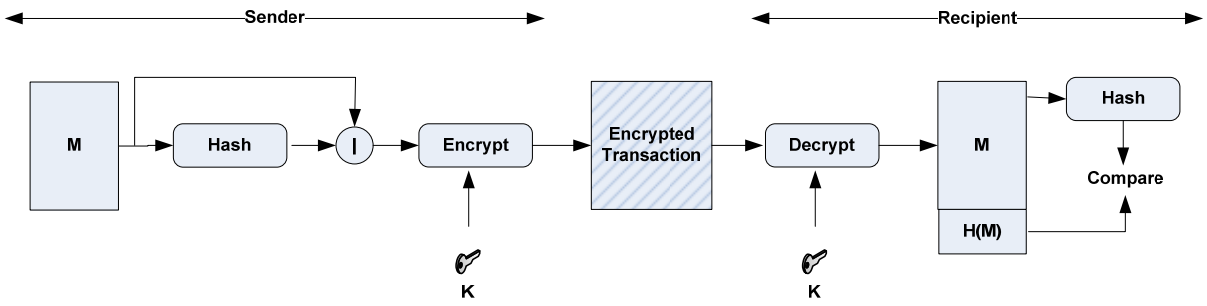

Figure 4. A Simplified Example of the Use of a Hash Function for Message Authentication with Confidentiality

Another technique is to encrypt the hash value which can be used as message authenticator as shown in Figure 5. The message and the message authenticator can be sent to the recipient. The recipient can decrypt the authenticator and can compare the resulting value with the one calculated.

If they are identical, the message has not been modified and was sent from the sender who shares the secret key.

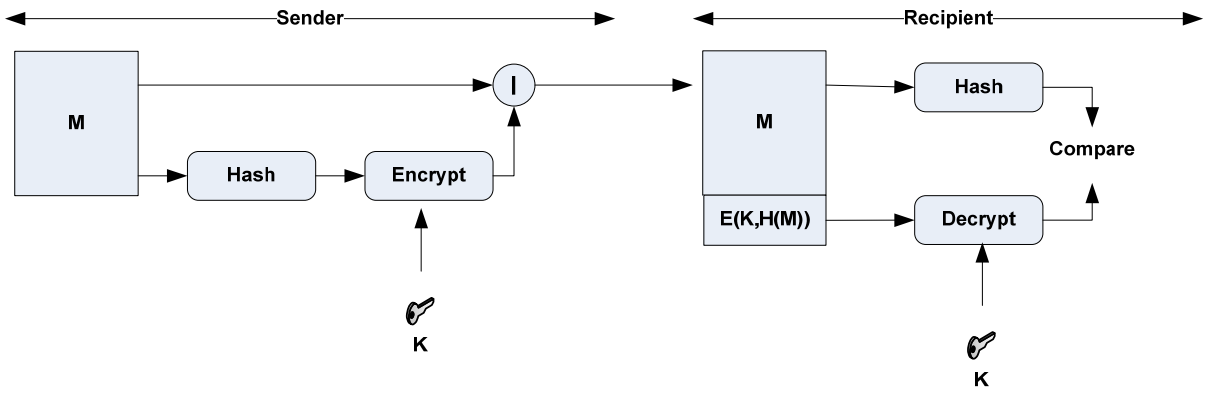

Figure 5. A Simplified Example of the Use of a Hash Function for Message Authentication without Confidentiality

Cryptographic hash algorithms that are in common use today include:

- Message Digest (MD): MD5 (RFC 1321) was developed by Rivest. MD5 has been implemented in a large number of products although several weaknesses in the algorithm have been discovered.
- Secure Hash Algorithm (SHA): The Secure Hash Algorithm is published by NIST as a U.S. Federal Information Processing Standard (FIPS). SHA-1 produces a 160-bit hash value and was originally published as FIPS 180-1 and RFC 3174. SHA-2 (FIPS 180-2) defines three new versions of SHA, with the hash value length of 256, 384, and 512 bits, known as SHA-256, SHA-284, and SHA-512, respectively. A revised document was issued as FIPS 180-3, which added a 224-bit version.

Hybrid Encryption

The most popular public key cryptography algorithms are several orders of magnitude slower than the best known secret key cryptography. Furthermore, at the same cryptographic strength, public key algorithms require a much larger key. However, secret key cryptography requires that the secret key to be shared between parties involved in communication. In order to mitigate the drawbacks, a hybrid scheme is needed. As illustrated in Figure 6, a session key is randomly generated and is used to encrypt the message using a secret key cryptography. This provides efficiency to the scheme. The session key is then encrypted using the recipient's public key. This is more convenient since both parties do not have to share a secret key. Both the encrypted message and the encrypted secrete key are transmitted to the recipient.

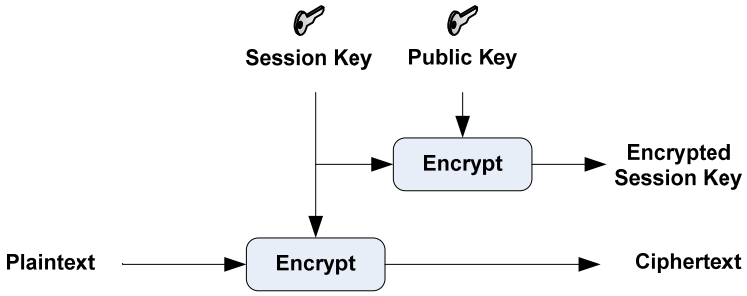

Figure 6. Hybrid Encryption

When the recipient received the secure transaction, the recipient can use the private key to decrypt the encrypted session key and can use the session key to decrypt the encrypted message to obtain the original message. The process of hybrid decryption is shown in Figure 7.

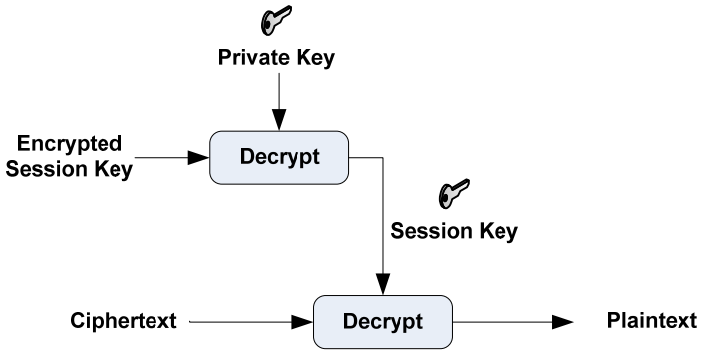

Figure 7. Hybrid Decryption

Digital Signatures

An author of the message can create a signature for the message. The signature for the message m can only be generated by someone with the knowledge of the author's private key and the signature depends on the contents of the message m. If the message is modified in any way, the signature no longer matches. Digital signatures provide integrity of the message and the authentication of the author. The author cannot repudiate the contents of the message being signed. Generating a signature on the message would be inefficient. Since the message digest depends on the message, signing the message digest is equivalent to signing the message and is more efficient. Figure 8 shows a simplified signature generation using message digest.

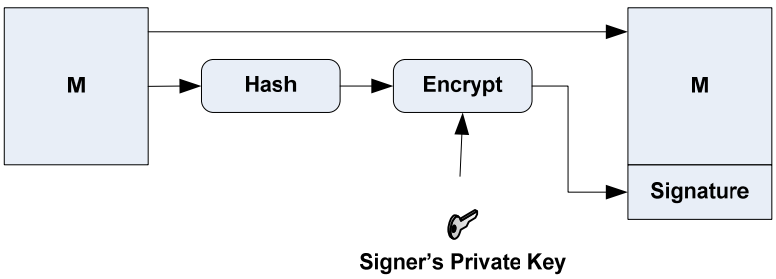

Figure 8. A Simplified Signature Generation Using Message Digest

Anyone can verify the signature by generating the message digest from the received message and can compare the generated message digest with the one obtained from decrypting the signature using the author's public key. The signature verification process is illustrated in Figure 9.

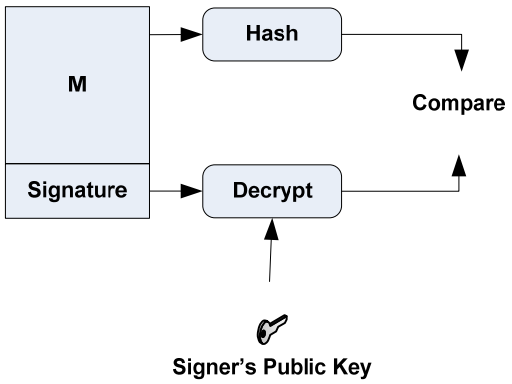

Figure 9. A Simplified Signature Verification Using Message Digest

Digital Signature Standard (DSS) [15] includes three techniques, namely; the Digital Signature Algorithm (DSA), the RSA digital signature algorithm, and the Elliptic Curve Digital Signature Algorithm (ECDSA) [16]. The security of the digital signature depends on the cryptographic hash function and the public key cryptographic algorithm. For breaking a digital signature, an attacker may create a fraudulent digital signature by creating a new message for an existing digital signature which is an attack on the cryptographic hash function or by constructing a fraudulent digital signature for a given message which is an attack on the public key cryptographic algorithm. The hash function must be collision resistant and the public key algorithm must be strong against attacks. The approved techniques are considered secure.

It is computationally infeasible to forge a digital signature. The digital signature provides authentication and non-repudiation. Therefore, if the signature is valid, the author of the message cannot deny creating the message.

2.6. Blind Signature Scheme

Blind signature [17] schemes can be used in applications where author privacy is important. The signing authority can certify certain information without revealing the information being signed.

A RSA signature is computed by raising the message *m* to the secret exponent *d* modulo the public modulus *n*. However, the blind version uses a random number *k*, such that *k* is relatively prime to *n*. *k* is raised to the public exponent *e* modulo *n*. The resulting value $k^e \ (mod\ n)$ is used as a blinding factor. The product of the message *m* and the blinding factor, $m' \equiv mk^e \ (mod\ n)$, can be sent to the signing authority. The blinded message m' does not leak any information about *m*. The signing authority computes the blinded signature as $s' \equiv (m')^d \ (mod\ n)$ and sends it back to the author of the message. The author of the message can remove the blinding factor to reveal the valid RSA signature of m as $s \equiv s' \cdot k^{-1} (mod\ n)$. The following equation proves that valid RSA signature of *m* can be obtained.

$$s \equiv s' \cdot k^{-1} (mod\ n) \equiv (m')^d k^{-1} \equiv m^d k^{ed} k^{-1} \equiv m^d k k^{-1} \equiv m^d (mod\ n)$$

This scheme can be used in the online lottery since the lottery information is needed to be certified and cannot be known to the signing authority.

Chapter 3 Examples of Secure Systems

3.1. Political Party Member Database System

The Election Commission of Thailand maintains the political party member database. This database is used to check whether or not a person belongs to a political party. According the Thai law, the membership status may allow or may disallow a person from doing certain things. For instance, a representative candidate must belong to a political party at least 30 days prior to the election date and a senator candidate must not have been affiliated with a political party in the last five years. Therefore, this database must be accurate and resilient against forgery and tampering. The system demands a high level of security requirements since it has a significantly high level of the potential impact. The data are used as the fundamental part of a democracy.

Political Party Member Information Certification

The information is time sensitive. Therefore, it must be certified by several authorities in order to have check and balance. This ensures that no information can be modified illegally. The system employs the use of digital signatures. Each record must be signed three times. First, the political party leader must certify that a person has applied for a membership and is qualified in accordance to the law by signing the member information. Second, an election commissioner must check and certify the information submitted by the political party. Third, another election commissioner must also check and certify the member information. The political party member record signing is shown in Figure 10.

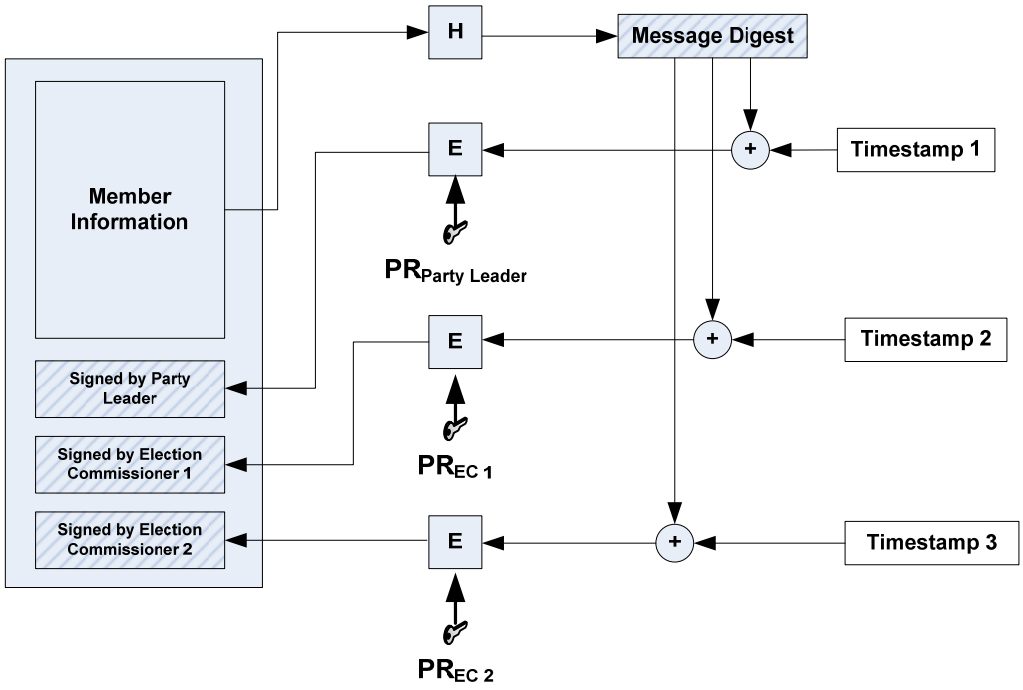

Figure 10. Political Party Member Record

Three signatures are required because this can provide a balance of power. It can prevent collusion at a certain level. The political leader cannot change the member information, recertify, and pay the system administrator to update the database. By doing so, it will cause signature verifications of both election commissioners to fail. The system also prevents any two signing authorities from colluding. The signature verification of the third signer will fail. However, if all three signing authorities collude, real-time verification would pass. It does not mean that the system totally fail at this point. Further security measures will be explained later.

Political Member Information Verification

With the use digital signatures, non-repudiation can be accomplished. The signing authorities cannot refuse certifying the information. The political party leader cannot refuse certifying the member information if the signature is valid. The election commissioners also cannot repudiate that the political party leader had submitted the member information record in timely manner. Even though the political party member database is maintained by the Election Commission of Thailand as the primary database and is considered as the only accurate database by law, the party can obtain a copy of certified records. In the event of a dispute, digital signatures can be used to verify the non-repudiation. The process of political party member record verification is illustrated in Figure 11.

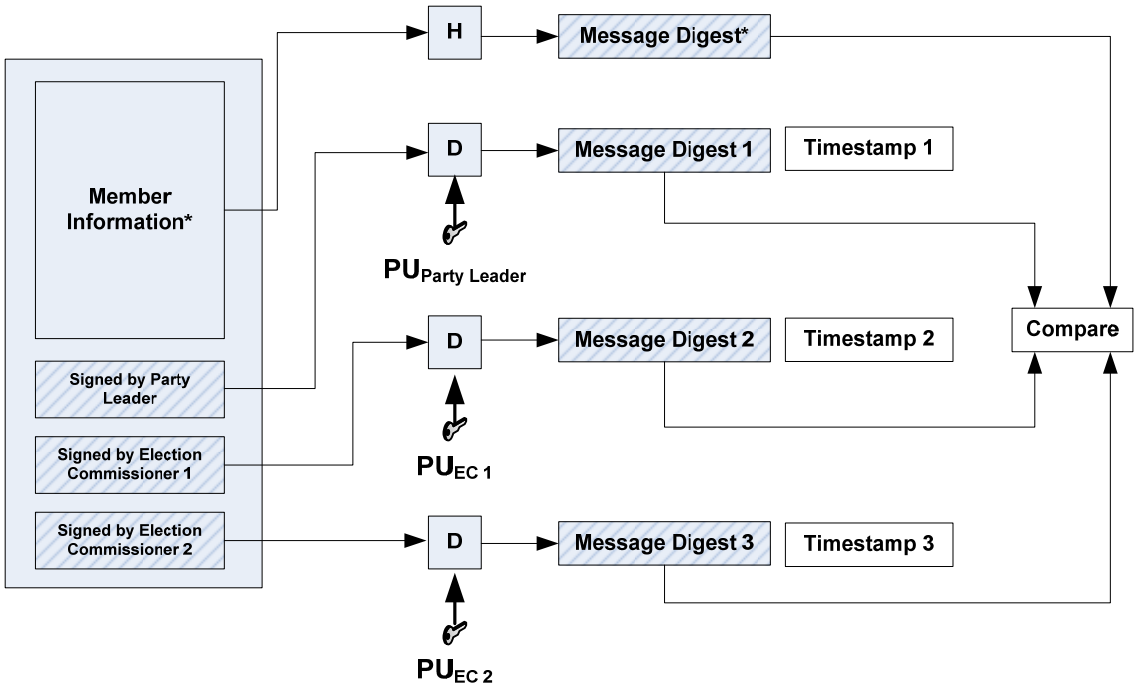

Figure 11. Political Party Member Record Verification

Encrypted Certified Political Member Information

After all three signing authorities have certified the political party member information and the information is published, another election commissioner randomly generates an encryption key to encrypt the published information and the encryption key is encrypted using the public key. The encrypted information is also signed. The signed encrypted information is stored as depicted in Figure 12. As mentioned earlier, if three signing authorities collude, this stored information can be used to settle the dispute.

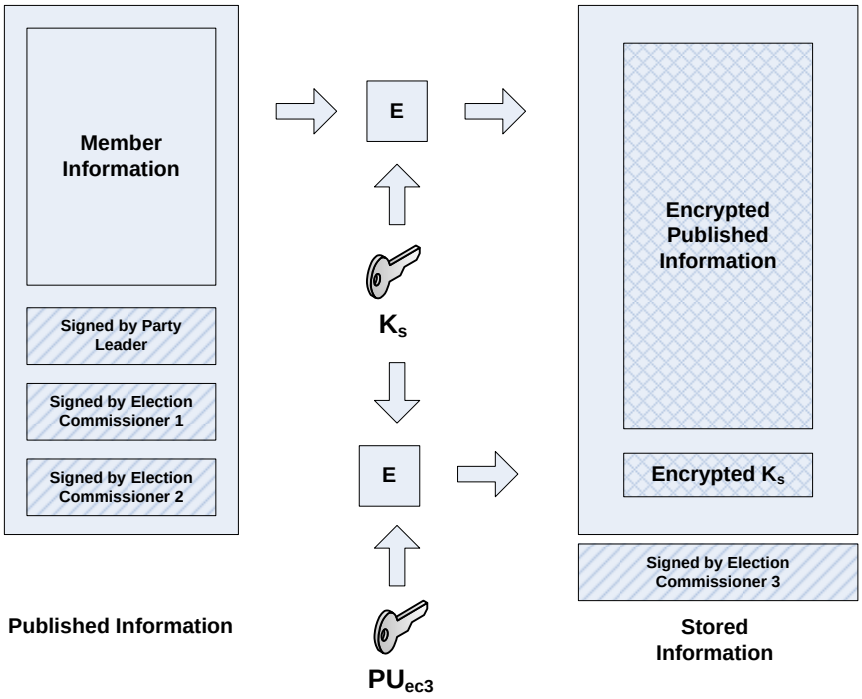

Figure 12. Encrypted Certified Political Member Information

The system not only uses cryptography to provide security, but it also employs other security measures such as a good security policy, host hardening, application hardening, network security, and backups.

3.2. Electronic Voting (E-voting)

Electronic voting or e-voting is a term encompassing several types of voting that uses electronic means of casting a vote and electronic means of counting votes. Electronic voting technology may include punch cards, optical scan voting systems, and specialized voting machines. Due to the rapid growth of computer networks and advanced in cryptographic technique, electronic polling will become a standard means of voting. Electronic surveys and elections can be inexpensive to administer. However, if not carefully designed, electronic polling systems can be easily compromised, thus corrupting results or violating voters' privacy.

In 1981, Chaum proposed the first published cryptographic voting protocol paper on anonymous electronic mail and digital pseudonyms [18]. This protocol uses public key cryptography and relies on rosters of digital pseudonyms to conceal the identity of voters. However, the protocol does not guarantee that the identity of voters cannot be traced. Subsequently, Chaum proposed a protocol which unconditionally conceals the identity of voters [19].

A security-conscious electronic polling system called Sensus [20] can be used to conduct surveys and elections over the Internet. Sensus was designed primarily as a replacement for postal mail balloting systems; however, it is flexible enough to suit a variety of other polling applications, including those not feasible using traditional polling systems.

Sensus Design Goals

The design goals of Sensus are based on a survey of the literature on traditional and proposed electronic polling system. It includes four core properties:

- Accuracy: A system is accurate if (1) it is not possible for a vote to be altered, (2) it is not possible for a validated vote to be eliminated from the final tally, and (3) it is not possible for an invalid vote to be counted in the final tally.
- Democracy: A system is democratic if (1) it permits only eligible voters to vote, and (2) it ensures that each eligible voter can vote only once.
- Privacy: A system is private if (1) neither election authorities nor anyone else can link any ballot to the voter who cast it, and (2) no voter can prove that he or she voted in a particular way.
- Verifiability: A system is verifiable if voters can independently verify that their votes have been counted correctly.

Sensus Polling Protocol

The pollster acts a voter's agent, presenting ballots to a voter, collecting the voter's response to ballot question, performing cryptographic functions on the voter's behalf, obtaining necessary validations and receipts, and delivering ballots to the ballot box.

The validator is responsible for checking voter registration and ensuring that each registered voter can only cast one vote. The validator certifies the vote by signing a blinded ballot. The voter then unblinds the validation certificate and submits it to the tallier along with the ballot. The validator will issue no more than one validation certificate to each registered voter.

The tallier is responsible for collecting the voted ballots and tallying the results of the election or survey. Voters first submit encrypted ballots, signed by the validator to the tallier. The tallier checks the authenticity of the validation and verifies that the encrypted ballot is unique among the encrypted ballots received thus far. If the ballot is valid and unique, the tallier issues a signed receipt to the voter. The voter then submits the ballot decryption key. The tallier uses the key to decrypt the ballot. After the election, the tallier publishes a list of encrypted ballots, decryption keys, and decrypted ballots, allowing for independent verification of election results.

The Sensus protocol overview is depicted in Figure 13.

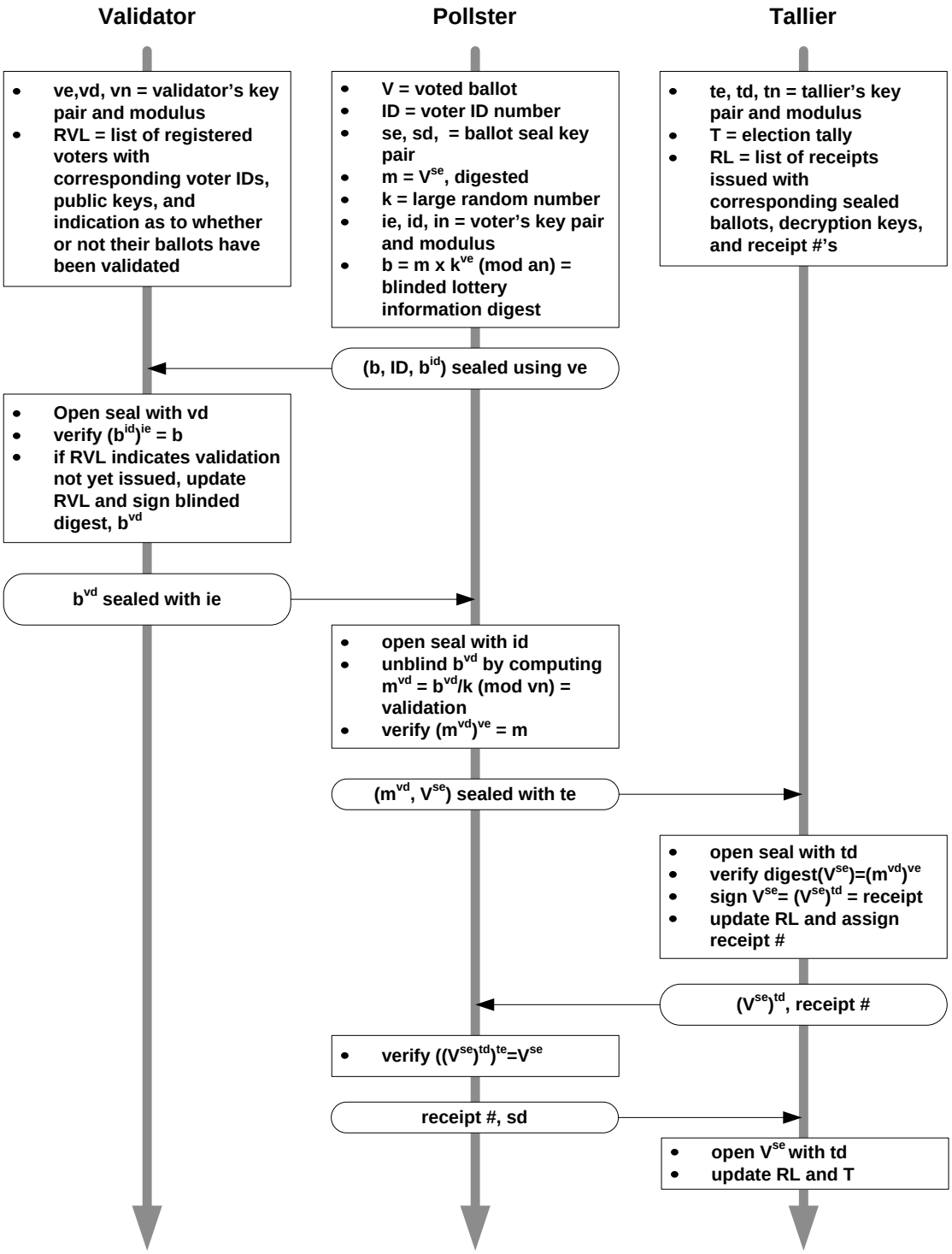

Figure 13. Sensus Protocol Overview

3.3. Korea Online E-Procurement System (KONEPS)

Korea's Public Procurement Service (PPS) established KONEPS as the national integrated e-Procurement system in September 2002 to enable the one stop service covering the entire online bidding process which includes bidding notice, bidding, contracting, inspection and tallying, and

payment request. The establishment and practice of KONEPS has been internationally recognized. PPS was awarded the Public Service Award (PSA) from the UN in 2003 and KONEPS was recognized as the Best Practice Model of e-Procurement in 2004. KONEPS also received the Global IT Excellence Award in the public field from WITSA. Furthermore, PPS has been visited by more than 50 countries which are interested in the implementation of e-Procurement of KONEPS.

PPS as a government procurement agency has three major roles, namely; minimization of government procurement costs, implementation of national policies in the real economy sector, and guarantee of transparency and fairness in procurement administration. Implementing e-Procurement has helped PPS achieve its goals to a certain extent. The e-Procurement has enhanced efficiency and transparency through the following:

- Reform of related laws and regulation
- Introduction of market competition
- Improvement of face-to-face contacts between government officials and procuring contractors
- Prevention of abuse of power by government officials
- Guarantee of administrative appeal for customers
- Reduction of paperwork
- Systematically management of documents
- Publication of information
- Sharing and co-use of information
- Publication of civil petition processing
- Integrated management of resources

In 2005, by using KONEPS, businesses and public institutions were able to reduce their procurement cost by 4.5 billion USD.

Architecture of KONEPS

KONEPS is a portal system that digitally processes complicated procedures and paperwork in public procurement. The main services of KONEPS include e-bidding, e-contract, e-payment and e-shopping. Figure 14 shows the architecture of KONEPS.

Followings are key functions of KONEPS:

- E-bidding: KONEPS publishes all bidding notices of public organizations such as governmental bodies, local autonomies and educational institutions through KONEPS.
- E-contract: KONEPS solves unnecessary suspicion and corruption factors during mutual contracts. The contract information is stored in the system, which upgrades the efficiency of procurement business and reduces the administration costs.
- E-payment: KONEPS provides real-time money transfer via linkage to the dBrain after payment request. Unnecessary documents for inspection/tally and online payment request were removed.
- E-shopping: KONEPS provides impartial opportunities to businesses and multiple choices to public organizations. Repetitive purchase and vexatious bidding process have been simplified via registration of the unit-price contract product and ordering function.

- Portal: KONEPS inquires the bidding information progress and legal information, introduces national contracts, searches work related library and conducts integrated searches for data. Provides information service, supports consulting, conducts surveys and provides online assistance.
- Integrated Bid Notice / Electronic Bidding: KONEPS manages the bid information posting, the biding results disclosure, integrated notice search, bidding-related info inquiry and supplier information.
- E-Procurement Application Service Provider: KONEPS requests purchase of goods, facilities and services, and manages contract delivery, inspection/review and invoicing.
- User Registration: KONEPS conducts registration by user (purchasers/suppliers), applies for bidding, inquires registration information by approver, manages users and approvers, and manages companies involved in unfair practices.
- E-Guarantee: KONEPS manages bidding guarantee, warranties, pre-payment guarantee, and agreements.
- Supplier's Performance: KONEPS inquires management status, credit rating, reference sites and engineers of suppliers.
- E-Payment: KONEPS manages general payment, payment by the government and payment by commercial banks.
- Document Distribution: KONEPS manages, preserves, provides, and converts electronic documents. Makes documents of related organizations connected.

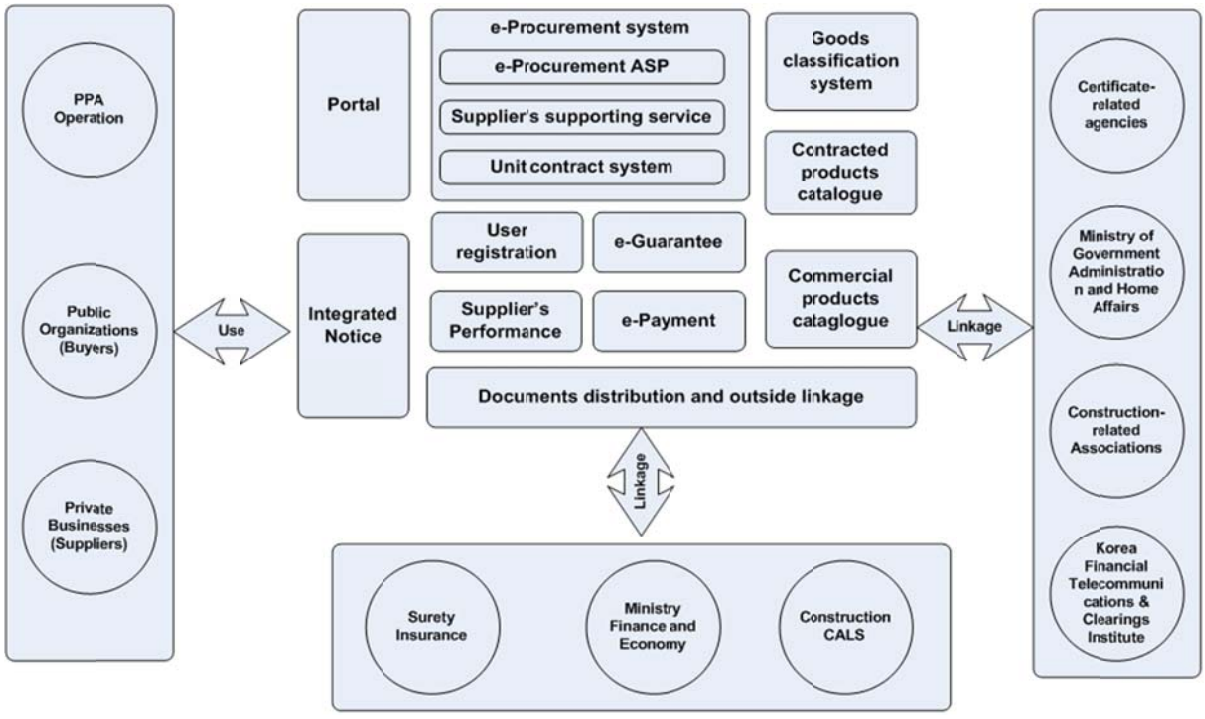

Figure 14. The Architecture of KONEPS

The Development of the Korean e-Procurement System

The development of the Korean e-Procurement System for centralized procurement consists of two parts; the development of the procurement EDI system and the development of the e-Bidding system which will be described below.

The development of the procurement EDI system:

EDI (Electronic Data Interchange) is the structured transmission of data between organizations by electronic means. It is used to transfer electronic documents from one computer system to another, i.e. from one trading partner to another trading partner.

Figure 15 illustrates the procurement process in the Korean public sector and the stakeholders involved in procurement administration.

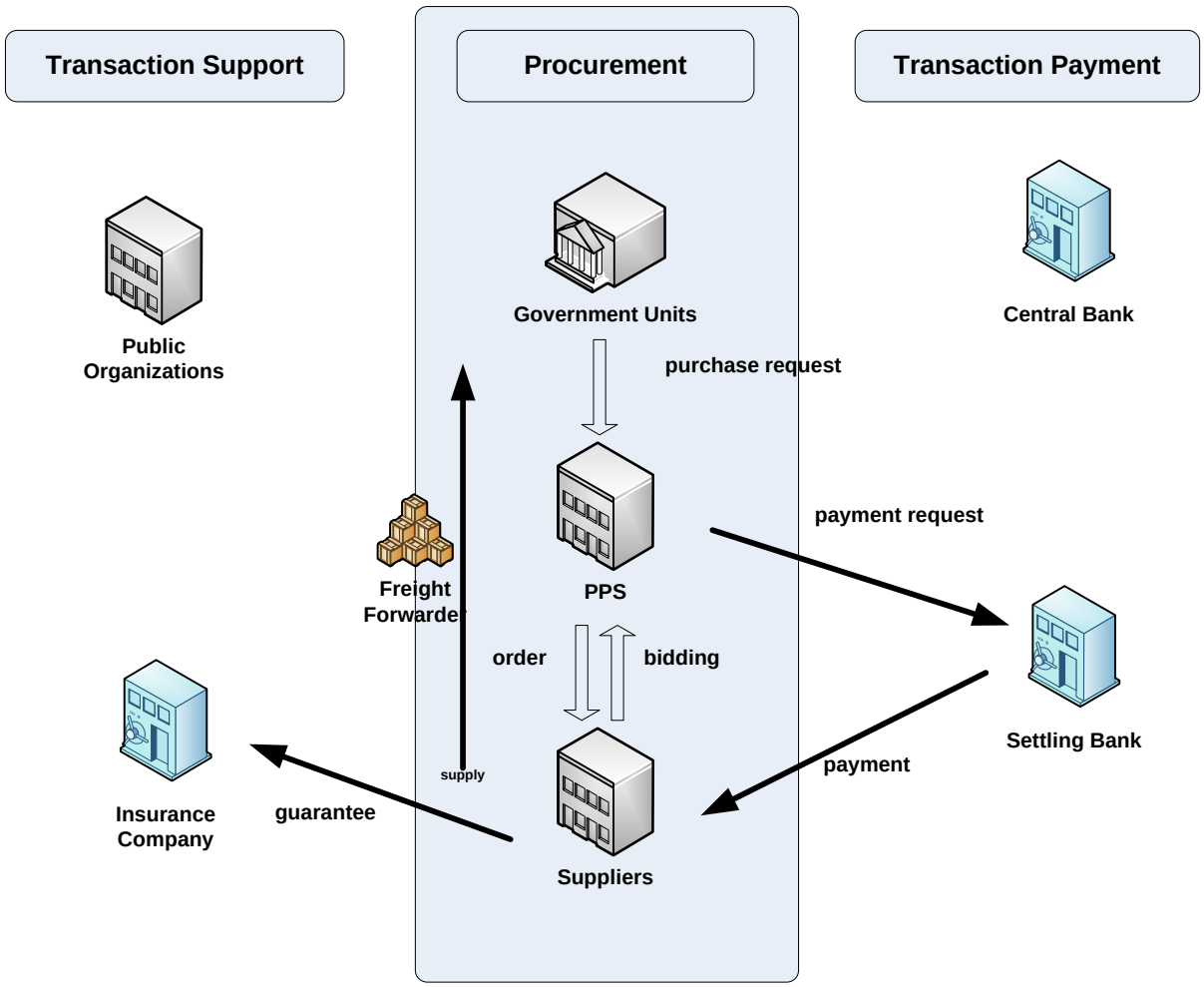

Figure 15. The Procurement Process in the Korean Public Sector and the Stakeholders

PPS receives procurement requests from demanding agencies, advises them of payment notices and delivery requests, and places the order with suppliers. Suppliers deliver orders to demanding agencies and receive payment via the Korean Central Bank from their settling banks.

The initial e-procurement system was based on EDI. Later on, the XML (eXtensible Markup Language) was adopted. KONEPS was developed with electronic documents based on the XML Schema from the World Wide Web Consortium (W3C) as well as the Core Component method from Electronic Business Extensible Markup Language (ebXML). Simple Object Access Protocol (SOAP) from Microsoft and ebXML Message Service Specification (MSS) are used for messaging. In addition, KONEPS employs the Universal Standard Products and Services Classification (UNSPSC) for commodity information and code management.

The development of the e-Bidding system:

In order to develop the e-Bidding system, the Korean Government has amended relevant laws and regulations. The e-Bidding system utilizes both symmetric and asymmetric key cryptography to ensure authentication, integrity, confidentiality, and non-repudiation. The symmetric key cryptography is used to encrypt large documents to ensure confidentiality whereas the asymmetric key cryptography is used to encrypt the secret keys and create digital signatures. Therefore, the Public-Key Infrastructure (PKI) must be available and the laws must define the legal validity of digital signatures.

Korea has a few Certificate Authorities (CAs), namely; KOSCOM, KICA, and NCA. These CAs provides public key certificates which can be used to authenticate the validity of the public keys of the entity involved in e-Procurement. Without a public key certificate issued by a designated certificate authority, bidding executives or suppliers are not allowed to participate in bidding. The e-Procurement system always connected to the CAs to confirm the validity of the certificate.

In e-Bidding, the bids must be kept secret until the deadline. To accomplish the bid secrecy, the secret key is issued by another authority. The NCA, a third-party government agency, issues an encryption key to every bid. When a bidding executive posts a bidding notice, bidders receive the encryption key and encrypt their bid using this key. Therefore, it is improbable that the bid can be opened without the encryption key. Even the PPS system administrators cannot regenerate an encryption key without the cooperation of the NCA or the bidding executive.

The e-Bidding system also supports the collection of bidding fees according to the conditions contained in the bidding notice. In such a case, the KFTC (Korea Financial Telecommunications & Clearings Institute) provides an Internet banking service that enables a transfer from a supplier's account to the noticing agency through the internet payment relay system. It is impossible to participate in the bidding without paying the fee. The bidding fees are for demanding agencies such as local governments and educational organizations who want to earn income from the bidding process due to their lack of local tax revenues. The e-Bidding process is illustrated in the figure below.

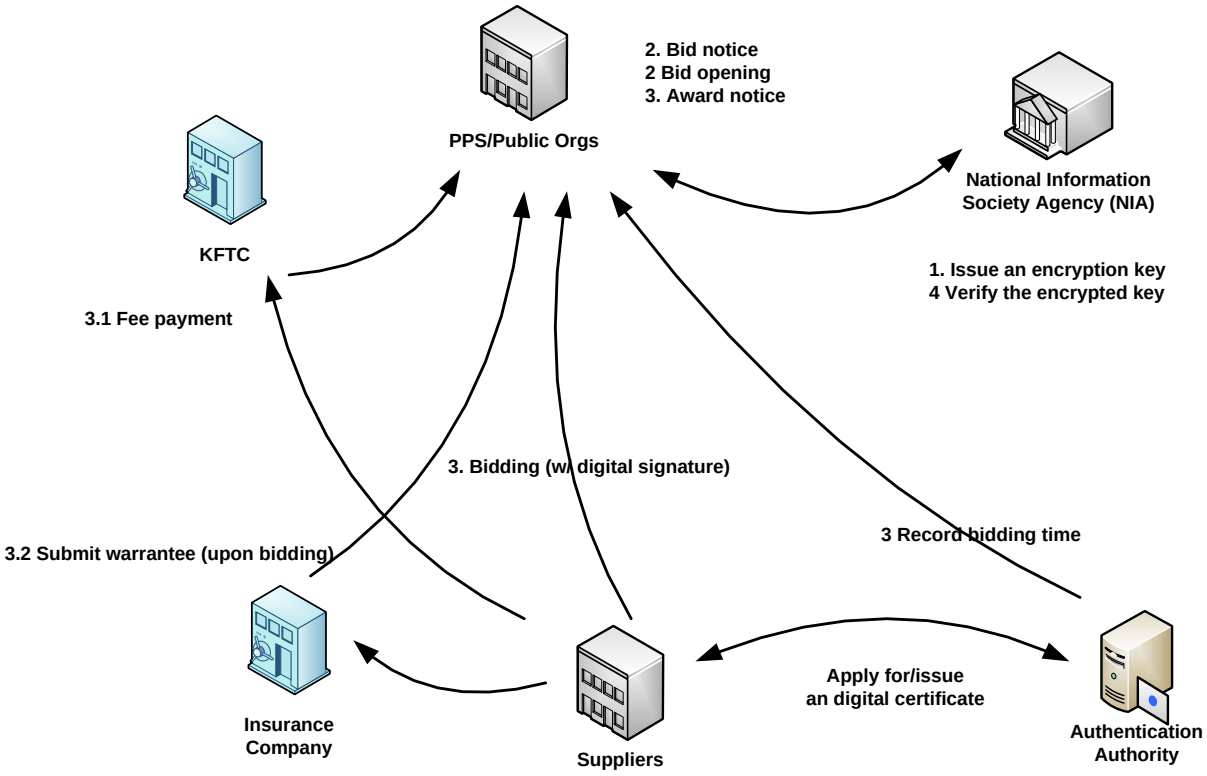

Figure 16. KONEPS E-Bidding Process

Chapter 4 Lotteries

A lottery is a form of gambling in which many people purchase chances to win a prize [6]. Some governments regulate or organize lottery, while others outlaw it. The first recorded signs of a lottery are dated back as early as between 205 and 187 B.C. during the Chinese Han Dynasty in what is now China. It is believed that the game called Keno, a lottery-like game, had helped finance major government projects like the Great Wall of China. References to lotteries have been found in many ancient texts from various civilizations such as Ancient China, Celtic, Ancient Greece, and the Roman Empire. The first European lotteries in the modern sense of the word appeared in 15th-century Burgundy and Flanders with towns attempting to raise money to fortify defenses or aid the poor.

The basic elements of modern lottery operations are recording the numbers and the amounts staked, drawing for determining the winning numbers, and collecting and pooling all the money placed as stakes. In a large-scale lottery, a computer system is used for recording purchases and printing tickets.

4.1. Types of Lotteries

The types of lotteries which are popular in many countries are conventional lottery, lotto, instant lottery, the number game, and Toto. The following section is the summary of each type of lottery.

1. Conventional lottery or the classic lottery: A limited numbers of lottery tickets are preprinted. Bettors must choose from available tickets.
2. Lotto: Bettors can choose a set of numbers. For example, a 6/49 lotto allows the bettor any six numbers out of 49 numbers.
3. Instant lottery: Tickets are preprinted and the prizes are predetermined. After the bettor buys the ticket, the bettor can reveal whether or not it is a winning ticket. Scratch-off tickets are popular instant lottery tickets.
4. The number game: Bettors can choose a number. For example, in a four digit lottery, the bettor can pick a number from 0000 to 9999. Winning tickets can match all digits in order or a different order, match the front pair or the back pair, and the like.
5. Toto: It is the lottery which is used to bet on sports. The tickets contain several matches. The bettor can choose the outcome of each match.

The lotto is the leading form of lottery in the world, with an annual total turnover in excess of $150 billion.

There are four types of user-selected number games, namely, one-number lottery games, multi-number lottery games, multi-number lottery games with two sets of numbers, and keno type lottery games [21]. All of which will be described briefly.

- One-number lottery games: The player selects just one number. For example, the number may have three or four digits.
- Multi-number lottery games: In these games, the player chooses a certain sets of numbers out of the numbers from one to a specified maximum number. Multi-number games are

usually denoted by the abbreviation n/N, which means that the player must select n numbers from 1 to N.

- Multi-number lottery games with two sets of numbers: For these games, the player must select from two sets of numbers. The games are denoted by the abbreviation n/N + m/M, which means that the player has to select n numbers from 1 to N from the first set and m numbers from 1 to M from the second set. For example, the Mega Millions is denoted by 5/56 + 1/46.
- Keno type lottery games: Similar to the multi-number lottery games, the player selects a set of numbers from the range of numbers. Unlike the multi-number lottery games, the player does not have to get all the selected numbers right in order to win the top prize.

In an online lottery system, tickets can be purchased using a lottery terminal. The tickets are recorded on the server and are printed out for the bettors. When the lottery is offered online, security is an important issue. The system must provide sufficient security services.

4.2. Electronic Lottery Schemes

Existing electronic lottery schemes proposal criteria that includes providing anonymity of bettors, randomized generation of the winning number, abilities to verify the winning number, and forge proof [22], [23]. In [22], the lottery number is revealed to the lottery authority.

Goldschlag and Stubblebine proposed a publicly verifiable lottery scheme based on a delaying function [24]. Each lottery ticket has an equal chance of being selected as a winning ticket. Since all information will be published, anyone can calculate the winning number based on the parameters of purchased tickets, and the winning number calculation is repeatable. Since the calculation uses a delaying function, nobody can get the result before the lottery closes. The winning ticket is selected among all purchased tickets. Therefore, each round must have a winner which is not suitable for a lottery scheme that allows rollover.

Kazue Sako presents an implementation of a digital lottery server as a Web application which offers an outcome that players can agree to be random [25]. The server allows users to define and start lottery sessions, participate in the session, and verify the outcome. The dealer initiates a lottery session on the lottery server. Each player chooses the session to participate in and submits a random string to the server. The server uses the submitted random strings among other parameters to calculate the result by using a cryptographic hash function. The outcome is published on the web, together with the players' random strings and other parameters. Each player can verify that the submitted random string was indeed included. However, this scheme places trust on the server. Should the server be compromised, the result could be altered.

Chapter 5 Protocol Design

This chapter presents the design of a secure online lottery system. First, the design objectives are defined. Then, the system design is presented. The system design consists of three parts, specifically, the design of lottery purchase process, the closing time process, and the verifying winning number process. Finally, the evaluation of the system is discussed.

5.1. Design Objectives

The following properties are the design goals of a secure online lottery system.

1. Accuracy: A system is accurate if it is not possible for the sold lottery numbers to be modified.
2. Privacy: A system is private if neither authorities nor anyone else can reveal the identity of the buyer without the buyer's consent.
3. Transparency: A system is transparent if it does not permit the authorities or anyone to obtain information from the system on the lottery numbers sold before the drawing and to add new numbers after the drawing.
4. Verifiability: A system is verifiable if the buyer can claim the winning number even the data in the system is completely destroyed.

5.2. Lottery Purchase Process

The secure online lottery system consists of three modules, namely; auditor, lottery terminal, and lottery authority. The auditor is the signing authority who ensures that the lottery system is conducted according to the policy. The responsibility of the auditor is to sign the purchased lottery information without having the knowledge of the information, to decrypt the session keys, and to release the session keys to the lottery authority when the lottery drawing has ended. The lottery terminal allows the player to buy a lottery ticket. The responsibility of the lottery terminal is to have the purchased lottery certified by the auditor and to submit the certified lottery to the lottery authority. Finally, the lottery authority is responsible for verifying the winning ticket.

Figure 17 shows the overview of the secure online lottery purchase protocol. The process is initiated when the buyer purchases a lottery. The lottery terminal acts as the buyer agent. The lottery information is hashed to obtain the message digest m. The obtained message digest is multiplied by the blinding factor as $k^{ae} \pmod{an}$. The blinded message digest and the signature are encrypted using the auditor's public key and sent to the auditor to be certified. The auditor cannot learn the lottery number being purchased. When the auditor receives the message from the lottery terminal, the auditor decrypts the message using the auditor's public key and verifies the signature of the lottery terminal. Upon successful verification, the auditor signs the blinded message digest. The signed blinded message digest is encrypted using the lottery terminal's public key and then is sent to the lottery terminal.

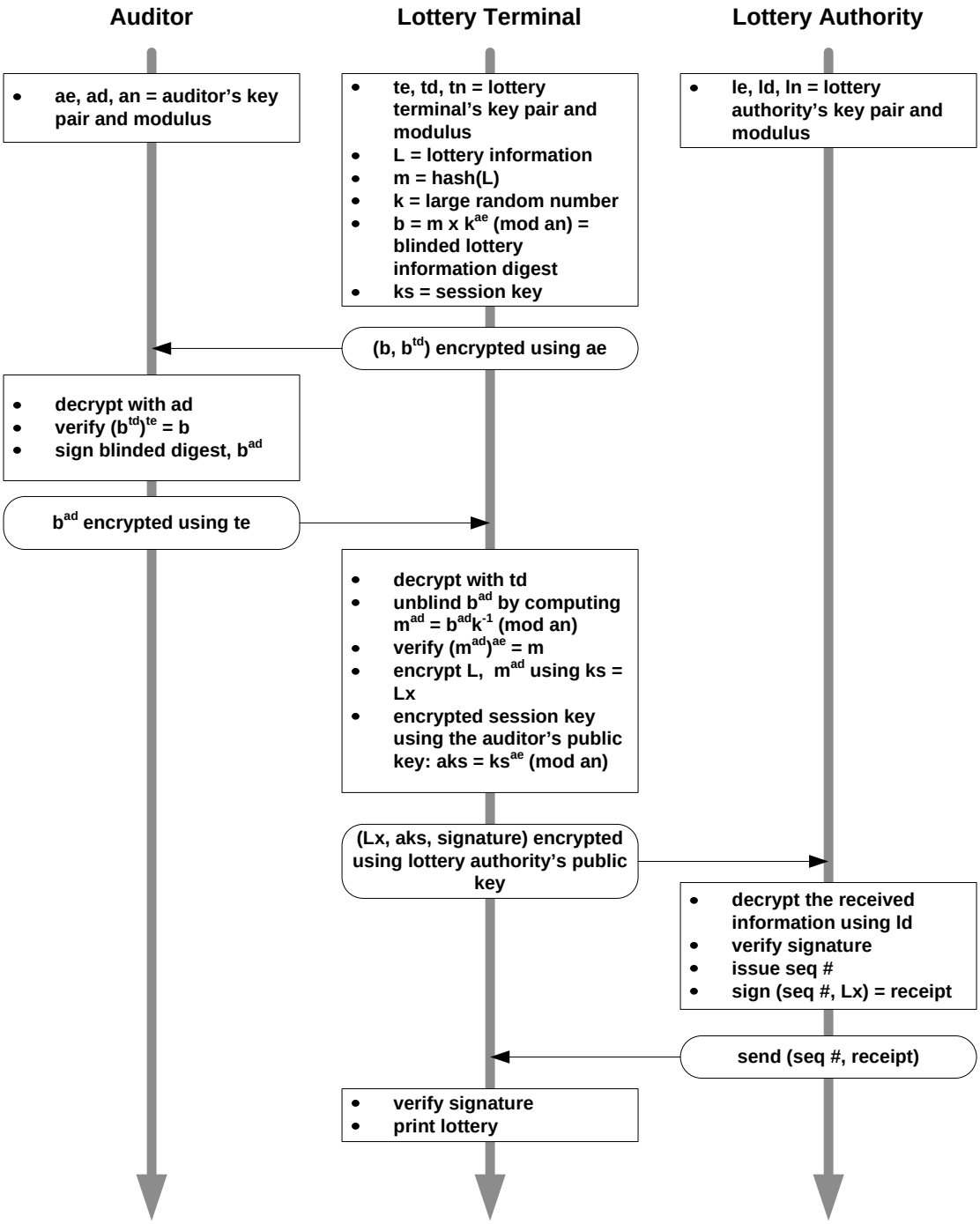

Figure 17. Secure online lottery purchase protocol overview

When the lottery terminal receives the message from the auditor, the lottery terminal decrypts the message using the lottery terminal's public key. The real signature of the auditor can be computed from the blinded signature. The lottery terminal also verifies that the signature is valid. After verifying the signature, the lottery terminal randomly selects a session key *ks* for the current lottery ticket. The lottery terminal encrypts the lottery information and the certified signature of the auditor using the session key. The session key is then encrypted using the lottery authority's public key. The encrypted certified lottery information, the encrypted session key and the transaction signature are encrypted using the lottery authority's public key and are sent to the lottery authority.

The lottery authority decrypts the received information using the private key and verifies the signature. Subsequently, the lottery authority issues a sequence number of the lottery ticket. A receipt for the lottery ticket is generated by signing the sequence number and the encrypted lottery information. The sequence number and receipt are then sent to the lottery terminal. The lottery authority does not know the lottery number since the session key is not available. It is encrypted using the auditor's public key.

When the lottery terminal receives the receipt from the lottery authority, the lottery terminal verifies the signature. After verifying the signature, the lottery terminal prints the lottery ticket. The bettor successfully purchases the lottery ticket. Note that the payment transaction description is omitted.

5.3. Closing Time Process

The auditor has certified all purchased lottery tickets and maintains a list of the corresponding sequence numbers and the encrypted session keys. However, the auditor does not have any knowledge of the purchased lottery numbers. On the other hand, the lottery authority has encrypted purchased lottery numbers and encrypted session keys, but the lottery authority cannot obtain any information on the purchased lottery numbers. This provides a balance of power between two authorities.

When the closing time has passed, the lottery authority publishes all sequence numbers along with the corresponding receipts and signs the published information. The lottery authority also sends the list of sequence numbers, encrypted session keys, and the receipts to the auditor. The auditor stops blind signing. The signature is verified.

After the all winning numbers have been drawn, the auditor sends a list of the sequence numbers and the session keys to the lottery authority. The lottery authority verifies the signature. For each lottery ticket, the lottery information together with the certified signature can be obtained using the corresponding session key. Then, the lottery authority verifies the signature. The closing time process is depicted in Figure 18.

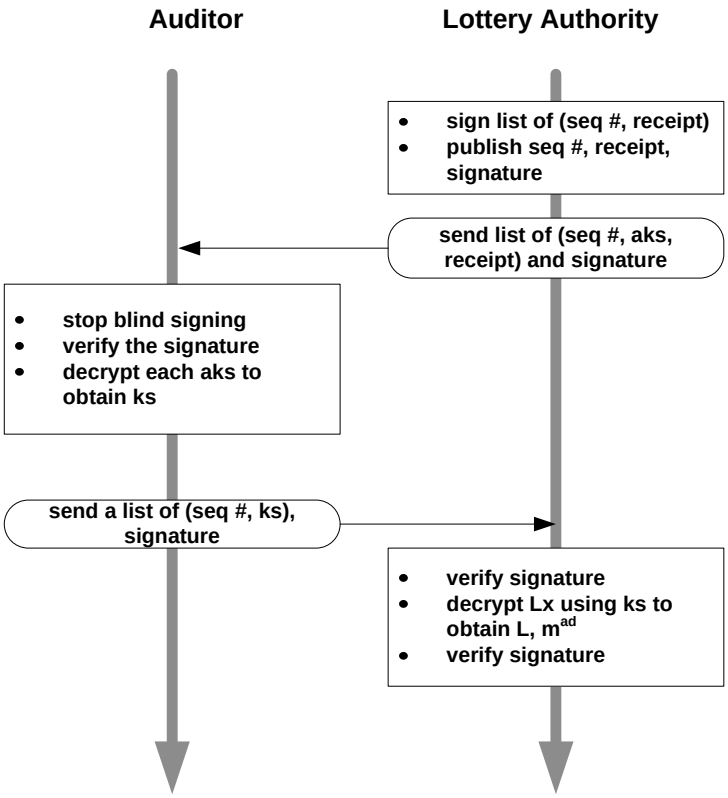

Figure 18. Closing time process

5.4. Verifying Winning Number Process

The bettor can check if the purchased lottery ticket is the winner by presenting the lottery ticket to the lottery terminal or the lottery authority. The lottery ticket is scanned to obtain information such as the sequence number, the lottery information, the certified signature, the receipt information, and the session key. The certified signature is verified by comparing the hash value of the lottery information with the value obtained from decrypting the signature using the auditor's public key. This ensures that the lottery ticket was certified properly. To verify the receipt information, the lottery information is encrypted using the session key *ks*. The hash of the sequence number and the encrypted lottery information is compared with the one obtained from decrypting the receipt using the lottery authority's public key. The last step is to compare the purchased lottery number against the winning numbers and display the result to the player. The process for verifying the winning number is illustrated in Figure 19.

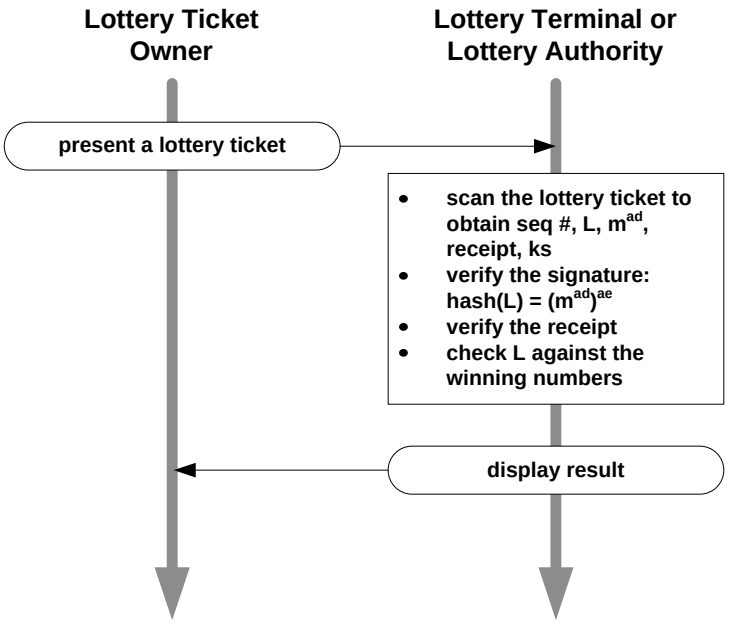

Figure 19. Verifying the winning number process

5.5. Evaluation

Four properties of the secure online lottery were given earlier. In this section, the secure online lottery system is evaluated accordingly. While evaluating the secure online lottery system, there are assumptions about other aspects of security that have been put into place. For example, the application security has been audited and the lottery terminal does not keep records on the sold lottery tickets.

Accuracy: The secure online lottery system satisfies the accuracy property. The sold lottery numbers cannot be modified. If they are modified, the signature verification will fail. If the auditor modifies the numbers and regenerates the signature, the receipt (the signature of the lottery authority) verification will not pass. Similarly, if the lottery authority modifies the lottery numbers and regenerates the receipt, the auditor's signature verification will fail. If both auditor and lottery authority collude, the modified receipt would not match any of the receipts published before the drawing.

Privacy: The secure online lottery system satisfies the privacy property well. There is no personally identifiable information collected. The owner of the ticket must possess the physical ticket to claim the winnings. At that time, the identity of the bettor is revealed.

Transparency: The secure online lottery system satisfies the transparency property to a certain extent. The auditor does not have knowledge about the sold lottery information. The lottery authority only has the encrypted lottery information. Therefore, neither authority can obtain information from the system on the lottery sold before the drawing. However, if both the auditor and the lottery authority collude, all lottery information can be revealed. The system can be designed to prevent this event by only storing the session key on the lottery ticket. However, it would be inconvenient to the lottery authority since the lottery authority will not have any information until the ticket owner comes forward to present the ticket. Even with collusion, no new

numbers can be added after the drawing without being detected since the lottery authority must publish all sequence numbers and receipts before the drawing.

Verifiability: The secure online lottery system satisfies the verifiability property. The purpose of this property is to protect the player from being denied from claiming the winning ticket. The lottery ticket contains both the auditor's and lottery authority's signatures. This provides non-repudiation from both authorities. However, if the data in the system is completely destroyed, there must be an investigation into the incident to ensure that no collusion occurred.

Chapter 6 Prototype of the System

A prototype of the secure online lottery system is implemented using Java programming language.

6.1. Architecture of the System

The system consists of three modules, namely; the auditor module, the lottery terminal module, and the lottery authority module. The auditor module and the lottery authority module are web services while the lottery terminal module is an application. The interactions between modules and web services are done using SOAP messages. The architecture of the secure online lottery system is shown in Figure 20.

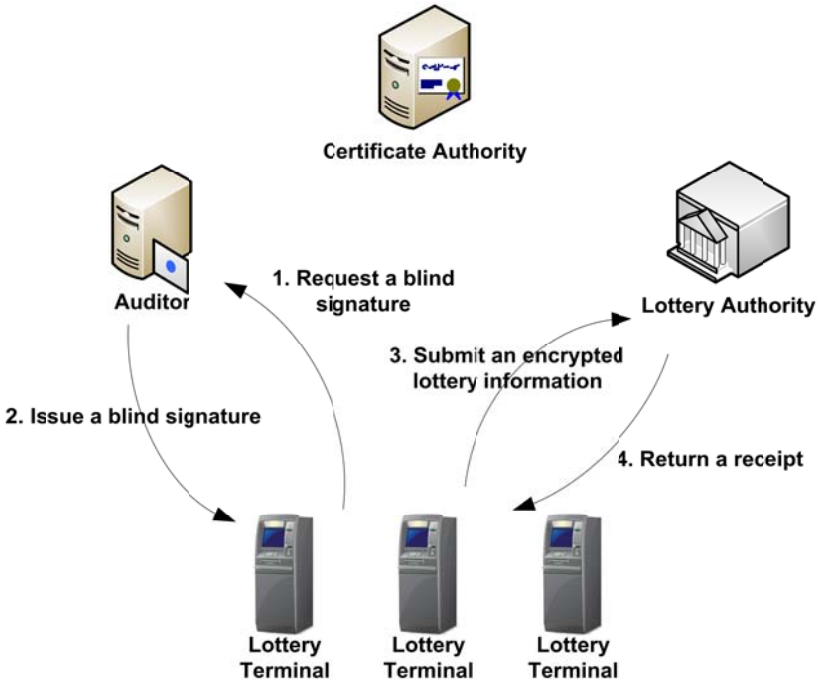

Figure 20. The architecture of the secure online lottery system

6.2. Cryptographic Library

Java Cryptography Architecture (JCA) for Java Platform Standard Edition 6 is used to implement the secure online lottery system. For symmetric cryptographic operations such as encryption and decryption, AES is used. The key length is 256 bits. However, RSA is used for asymmetric cryptographic operations that enable the encryption and decryption of data, and signing and verifying signatures. The key length is 2048 bits.

6.3. Printing Lottery Ticket

Human readable information such as the lottery numbers, the date, and the lottery period are printed on the lottery ticket. This is for the player to read only. The lottery ticket information which include the lottery number, data, lottery period, sequence number, certified signature, receipt, and

the session key are stored in a two-dimensional barcode [26], specifically the QR Code [27]. This provides a convenient way to transfer data from the lottery ticket to the lottery verification program by scanning the QR Code. Since the QR Code includes error correction, correct reading can be achieved even though a portion of the barcode is damaged.

Chapter 7 Conclusion

The online lottery system can be implemented in a secure manner through four desirable properties which include accuracy, privacy, transparency, and verifiability. The system is accurate since it is not possible for the sold lottery numbers to be modified. The privacy of the player is protected since no personally identifiable information is included in the lottery information. The system is transparent since it does not allow anyone to obtain the information of sold lottery numbers or to add new lottery tickets after the drawing. Finally, the system is verifiable since the buyer can claim the winning number even the data in the system is completely destroyed. Therefore, through this system, the lottery operation of the government can be transparent.

References

[1] Title 44 of the United States Code § 3542 (b) (1), United States Government Printing Office.

[2] U.S. Department of Commerce/National Institute of Standards and Technology (NIST), Standards for Security Categorization of Federal Information and Information Systems (FIPS PUB 199), 2004.

[3] "What is good governance?" UNESCAP, 2009. [Online]. Available: http://www.unescap.org/pdd/prs/ProjectActivities/Ongoing/gg/governance.asp [Accessed Oct. 7, 2009].

[4] World Lottery Association, "The World Lottery Association Values", [Online]. Available: http://www.world-lotteries.org/ [Accessed Aug. 5, 2012].

[5] The Internet Engineering Task Force (IETF), Internet Security Glossary (RFC 2828), May 2000.

[6] "lottery," in Encyclopædia Britannica 2009. [Online]. Available: Encyclopædia Britannica Online, http://www.britannica.com/EBchecked/topic/348555/lottery [Accessed: Aug. 5, 2012].

[7] The International Telecommunication Union (ITU), Data Communication Network: Open Systems Interconnection (OSI); Security, Structure and Applications, 1991.

[8] C. Kaufman, R. Perlman, and M. Speciner, *Network Security: Private Communication in a Public World*, 2nd ed. Upper Saddle River, NJ: Prentice Hall PTR, 2002.

[9] W. Stallings, *Cryptography and Network Security*, 4th ed. Upper Saddle River, NJ: Prentice Hall, 2006.

[10] J. Katz and Y. Lindell, *Introduction to Modern Cryptography: Principles and Protocols*, New York: Chapman & Hall/CRC, 2007.

[11] U.S. Department of Commerce/National Institute of Standards and Technology (NIST), Data Encryption Standard (DES) (FIPS PUB 46-3), 1999.

[12] A. Hevia and M. Kiwi, "Strength of Two Data Encryption Standard Implementations Under Timing Attacks," ACM Transactions on Information and System Security, vol. 2, no. 4, pp. 416–437, Nov. 1999.

[13] U.S. Department of Commerce/ National Institute of Standards and Technology (NIST), Advanced Encryption Standard (AES) (FIPS PUB 197), 2001.

[14] RSA Cryptography Standard, PKCS #1 v2.1, (2002)

[15] Digital Signature Standard (DSS), FIPS PUB 186-3, 2009

[16] Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), ANSI X9.62-2005.

[17] D. Chaum, "Blind Signatures for Untraceable Payments" in Advances in Cryptology: Proceedings of Crypto, pp. 199-203, 1982.

[18] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms", Communications of the ACM 24, 2 (1981), 84–88.

[19] D. Chaum, "Elections with unconditionally-secret ballots and disruption equivalent to breaking RSA," in Advances in Cryptology - EUROCRYPT '88 (Berlin, 1988), C. G. Gunther, Ed., vol. 330 of Lecture Notes in Computer Science, Springer-Verlag, pp. 177–182.

[20] L.F. Cranor and R.K. Cytron, “Sensus: a Security-Conscious Electronic Polling System for the Internet,” in Proceedings of the Thirtieth Hawaii International Conference on System Sciences, vo. 3, pp. 561-570, 1997.

[21] Common Types of Lottery Games. [Online]. Available: http://betstarter.com/lottery/LotteryGames.asp [Accessed: Aug 4, 2012].

[22] J. Zhou and C. Tan, “Playing Lottery on the Internet,” in Information and Communications Security, Lecture Notes in Computer Science, vol. 2229/2001,Springer, 2001, pp. 189-201.

[23] Y. Liu, et al., “A New Efficient E-Lottery Scheme Using Multi-Level Hash Chain,” in International Conference on Communication Technology, 2006, pp. 1-4.

[24] D. M. Goldschlag and S. G. Stubblebine, “Publicly verifiable lotteries: Applications of delaying functions,” Lecture Notes in Computer Science, Proceedings of 1998 Financial Cryptography, pp. 214-226, vol. 1465, 1998.

[25] K. Sako, “Implementation of a digital lottery server on WWW,” Lecture Notes in Computer Science, Proceedings of CQRE’99, pp. 101-108, vol. 1740, 1999.

[26] J. Z. Gao, L. Prakash, R. Jagatesan, “Understanding 2D-Barcode Technology and Applications in M Commerce–Design and Implementation of a 2D Barcode Processing Solution” in 31st Annual International Conference on Computer Software and Applications, pp.49-56, vol. 2, 2007.

[27] QR Code, http://www.denso-wave.com/qrcode/

สถาบันบัณฑิตพัฒนบริหารศาสตร์

118 ถนนเสรีไทย คลองจั่น บางกะปิ

กรุงเทพมหานคร 10240

โทร : 662-375-8972

โทรสาร: 662-374-2759

E-mail : rcadmin@nida.ac.th

© 2556 โดยสถาบันบัณฑิตพัฒนบริหารศาสตร์

สงวนสิทธิ์ : *ลิขสิทธิ์เป็นของผู้วิจัย และสถาบันบัณฑิตพัฒนบริหารศาสตร์ มีสิทธิ์นำไปเผยแพร่ได้ หากผู้วิจัยจะนำไปเผยแพร่ต้องระบุว่าได้รับทุนจากสถาบันบัณฑิตพัฒนบริหารศาสตร์*

ข้อความและความคิดเห็นใด*ในสิ่งพิมพ์ฉบับนี้ เป็นของผู้เขียน/คณะวิจัย มิใช่ของสถาบันบัณฑิตพัฒนบริหารศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์ ขอสงวนสิทธิ์ที่จะไม่รับผิดชอบต่อความเสียหายที่เกิดขึ้นกับบุคคลหรือทรัพย์สินอันเป็นผลมาจากสิ่งใดในรายงานฉบับนี้*