Electronic Payment System in Korea

May 2010

Mr. Youngchul Kang
CEO, NAISS
asia44@chol.com
Tel : 82-11-233-9610

NAISS

Defining NAISS

- Established in *2007*
- *NAISS* stands for 『National Administration Information System & Security』
- Construction of Korean E-Government Project (National Administration Information System) in *1980'*
- Building Telecom Network (Fixedline & Wireless) in *1990'*
- CEO of KICA (Korea Information Certificate Authority) & Co-chairleader of Business & Application WG of ASIA PKI Forum in *2000'*
- Adviser of e-payment Forum and Direct Load Control of electricity Forum

Contents

I. PKI and Digital Signature

1. What is PKI ?
2. Digital Signature

II. Large-Value Payment System (RTGS) in Korea

1. Outline
2. Main Functions of BOK-Wire
3. Intraday Liquidity Management
4. Management
5. Next Generation of BOK-Wire

III. Retail Payment systems (ACH) in Korea

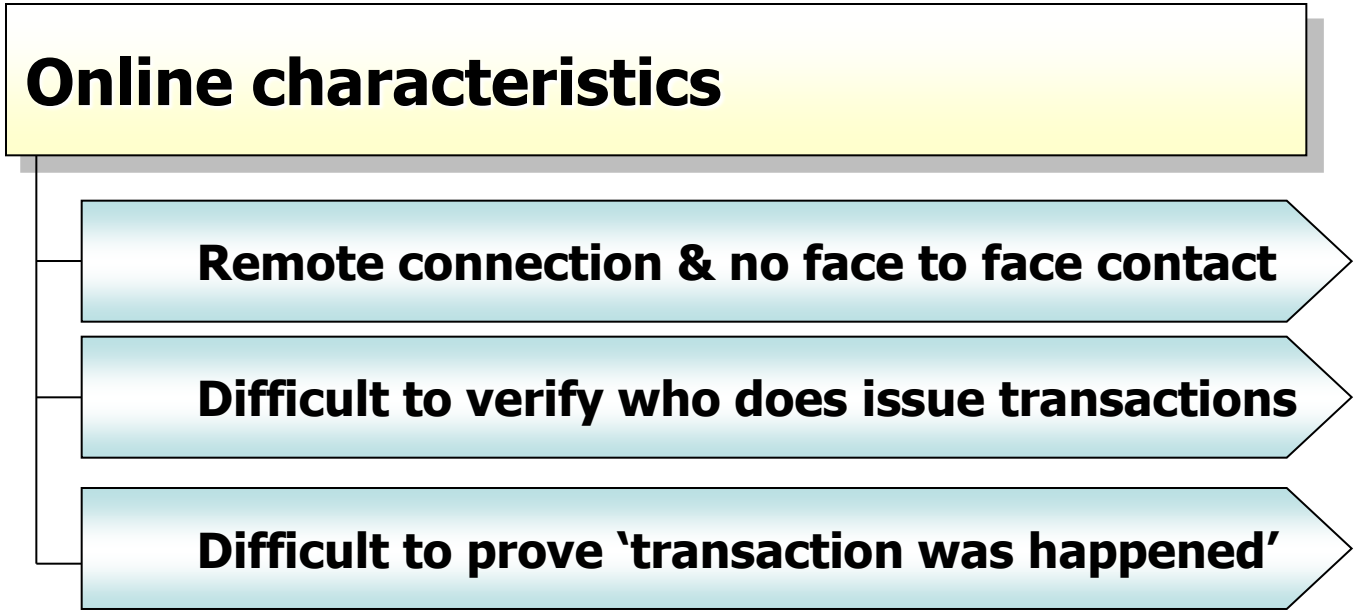
1. Outline
2. Check clearing System
3. Bank Giro System
4. Interbank Funds Transfer (IFT) System
5. Interbank CD/ATM System
6. Electronic Funds Transfer at the Point of Sale System
7. Electronic Banking System

NAISS

I. PKI and Digital Signature

1. What is PKI ?

Issued problems of e-Commerce



- Risk of breach about transactions and personal profile
- Difficult to secure transmitted contents
- Easy to make forgery document / Difficult to prove electrical document is in original state

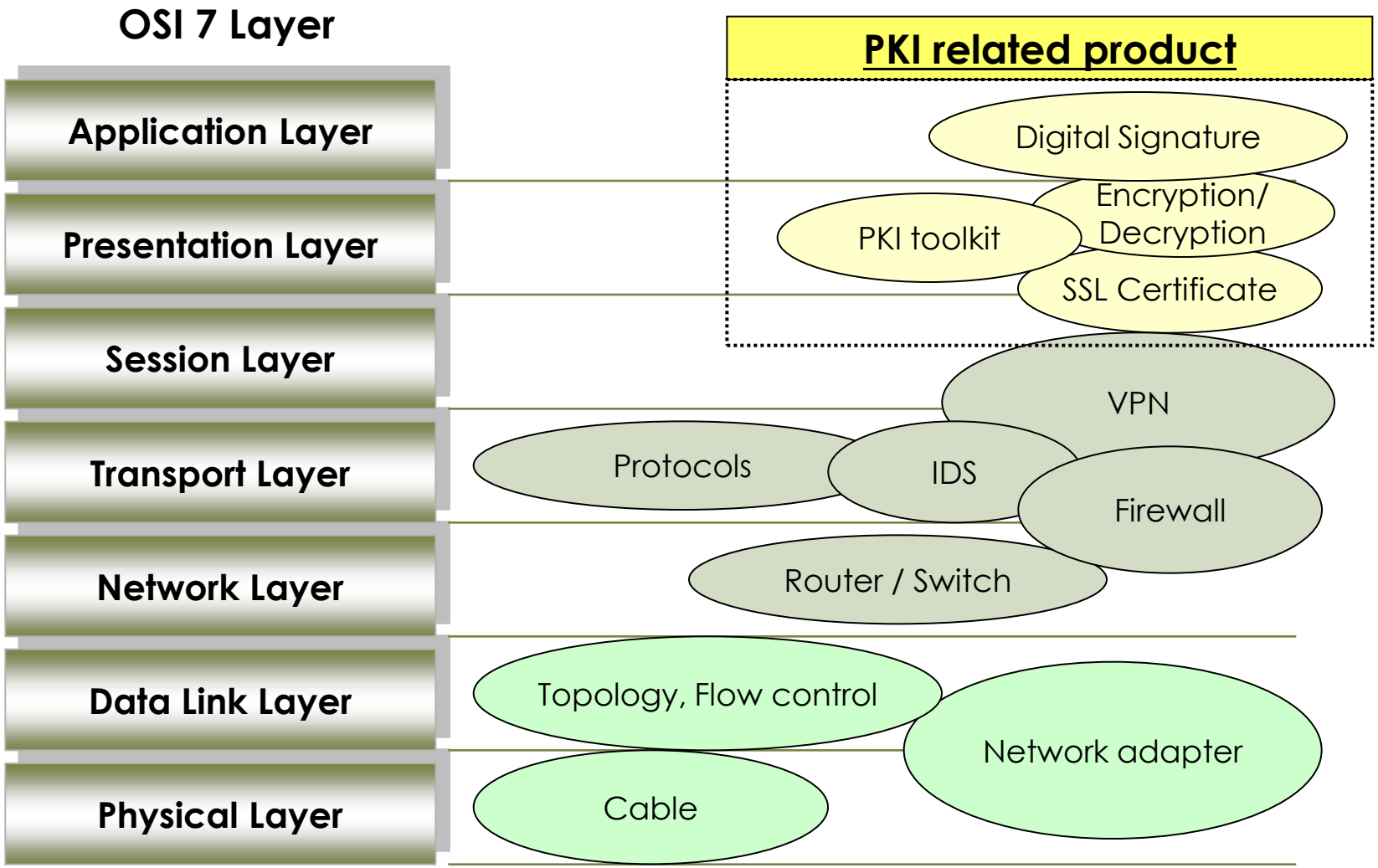
Possible Security Holes

- Breach of personal profile and credit card information at transaction
- Breach of personal profile in shared computer
- Cyber stealing
- Hacking on cyber securities & bank account / Stock price manipulation
- ID and password stealing

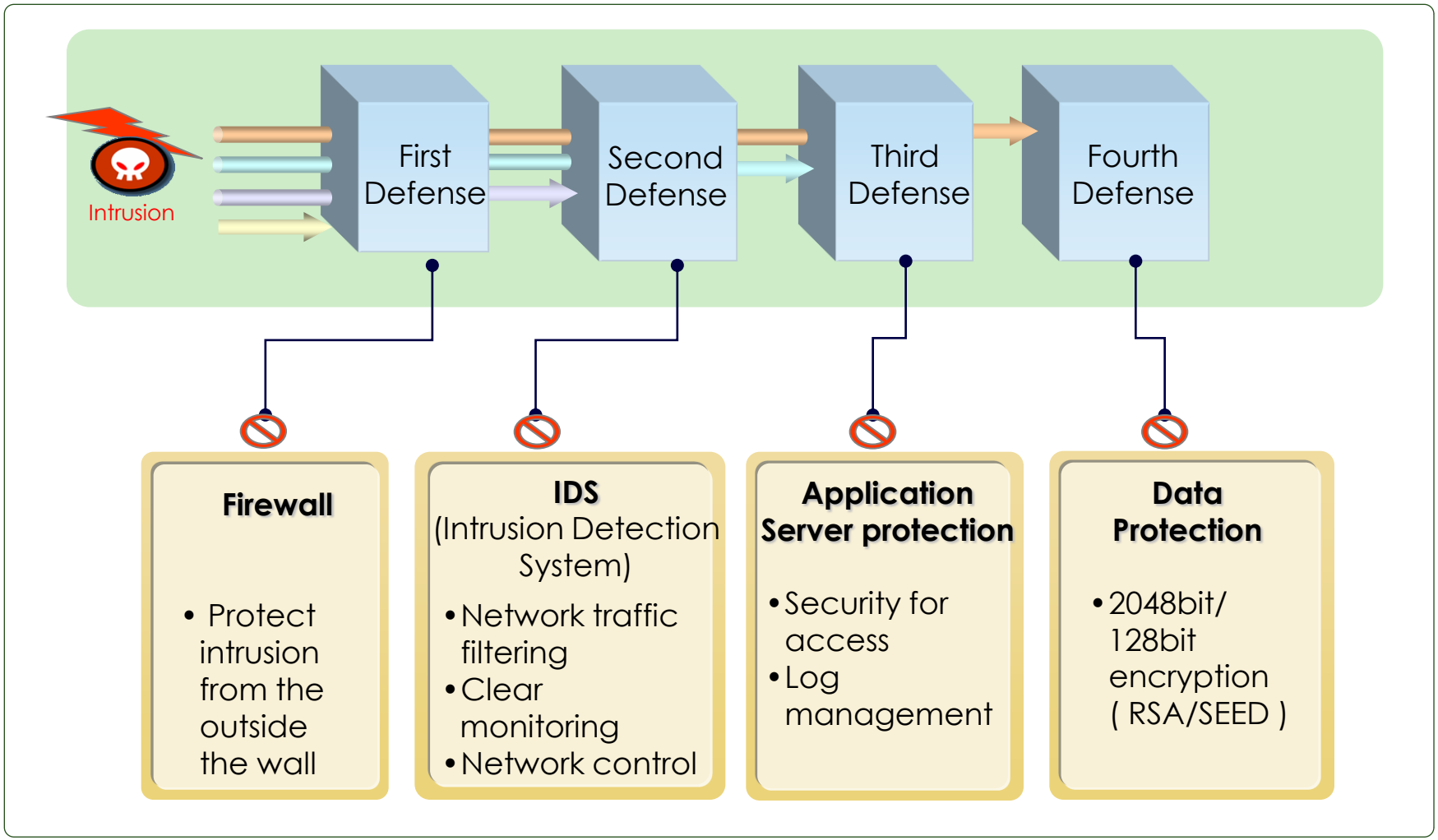
Need of Strong Security Protection
with PKI technology

NAISS

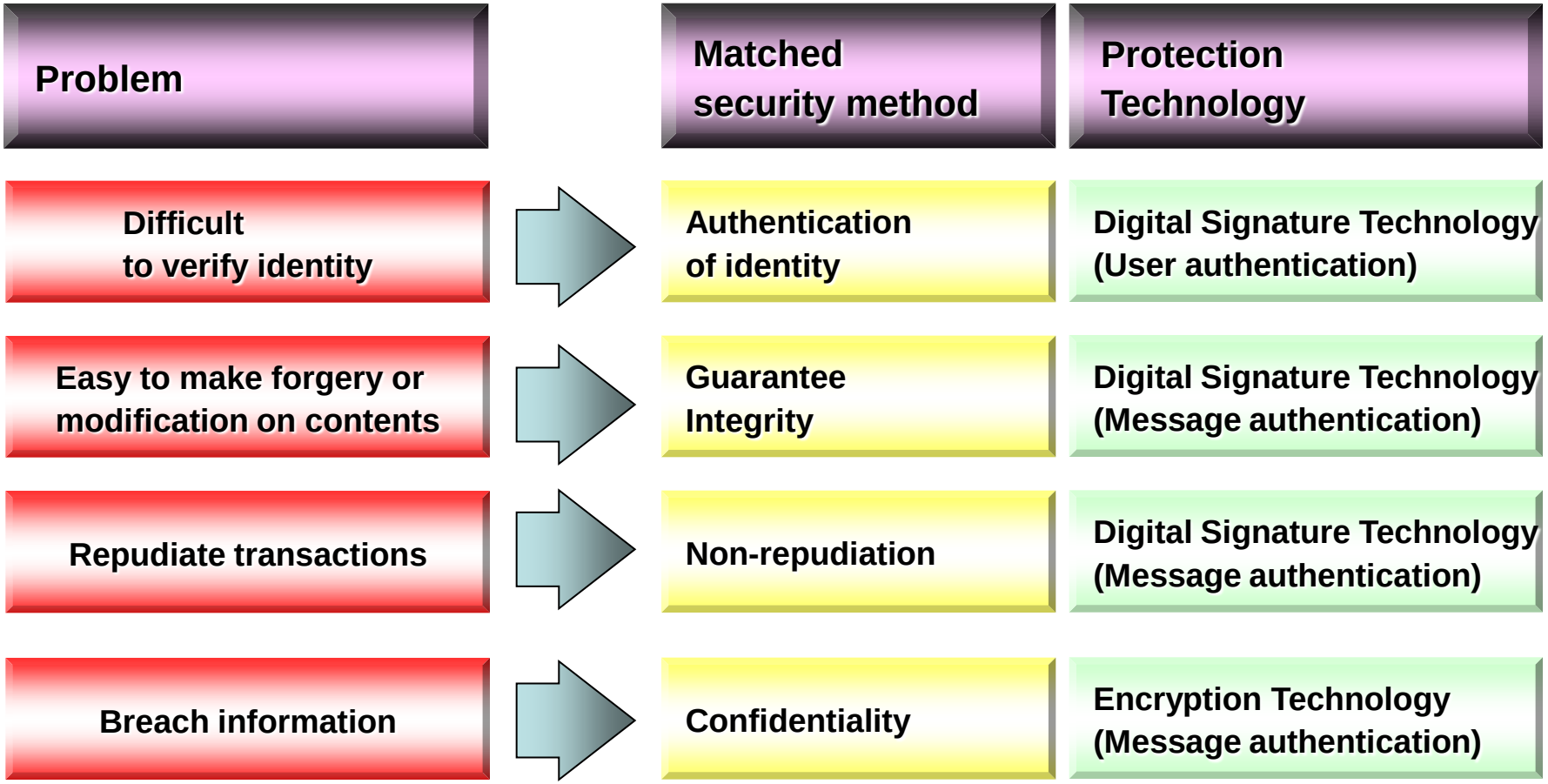
OSI Level matched Diagram



Simplified Security Diagram



PKI Solution to Hacking attempts



NAISS

Strong protection => PKI solution

PKI (Public Key Infrastructure)
The solution to exchange data securely using a pair of public key and private key in insecure public open network like Internet

PKI asymmetric sys.

Digital Signature with Private Key of user

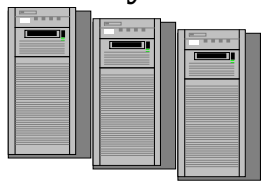
Internet

PKI asymmetric way

Encryption

Use Different Keys

Verify the signature with Public Key of user



Same ID / Password

Symmetric way

Encryption

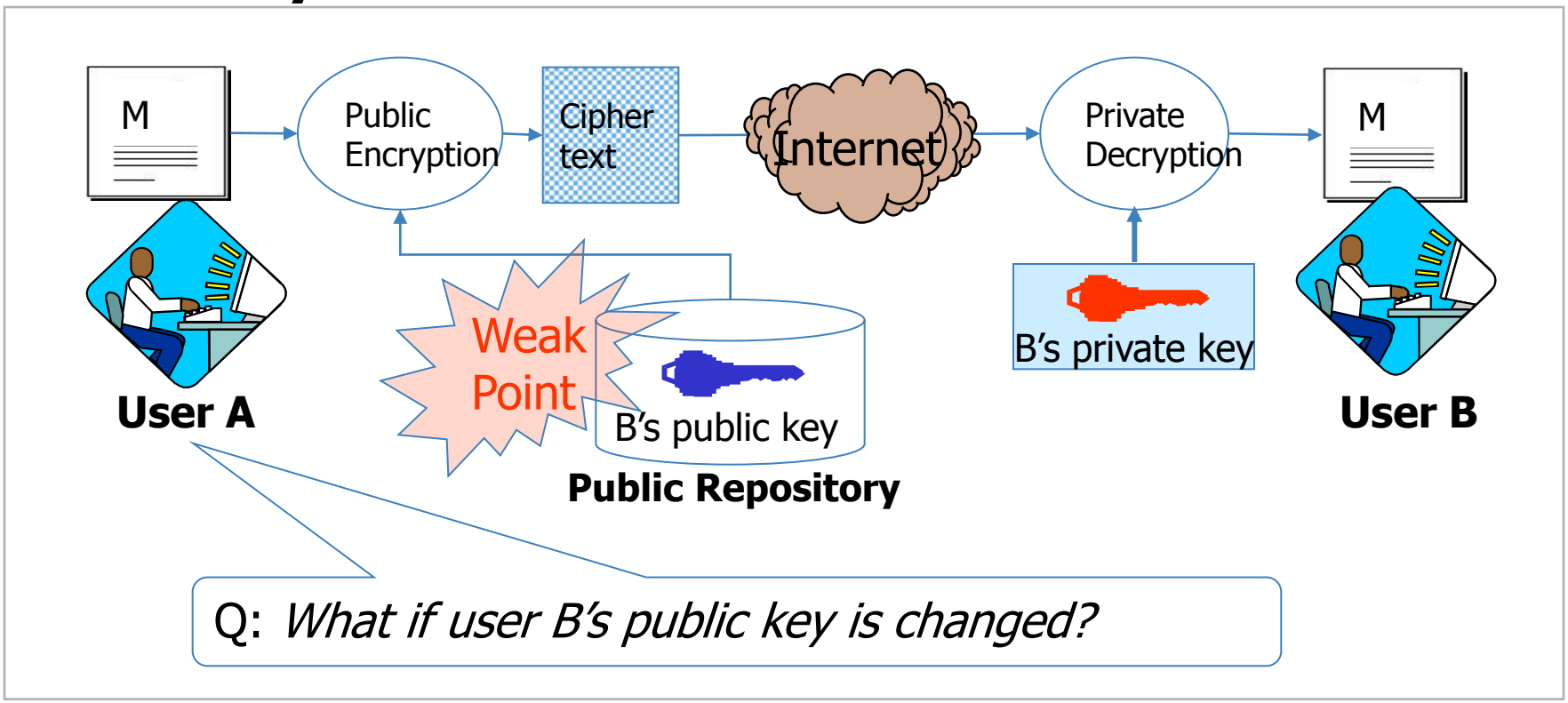
Symmetric system

Verify with same ID and Password;
ID and password is the key to access system

Symmetric Key
Share same ID and password on both sides

Appearance of CA

Public Key → Certificate

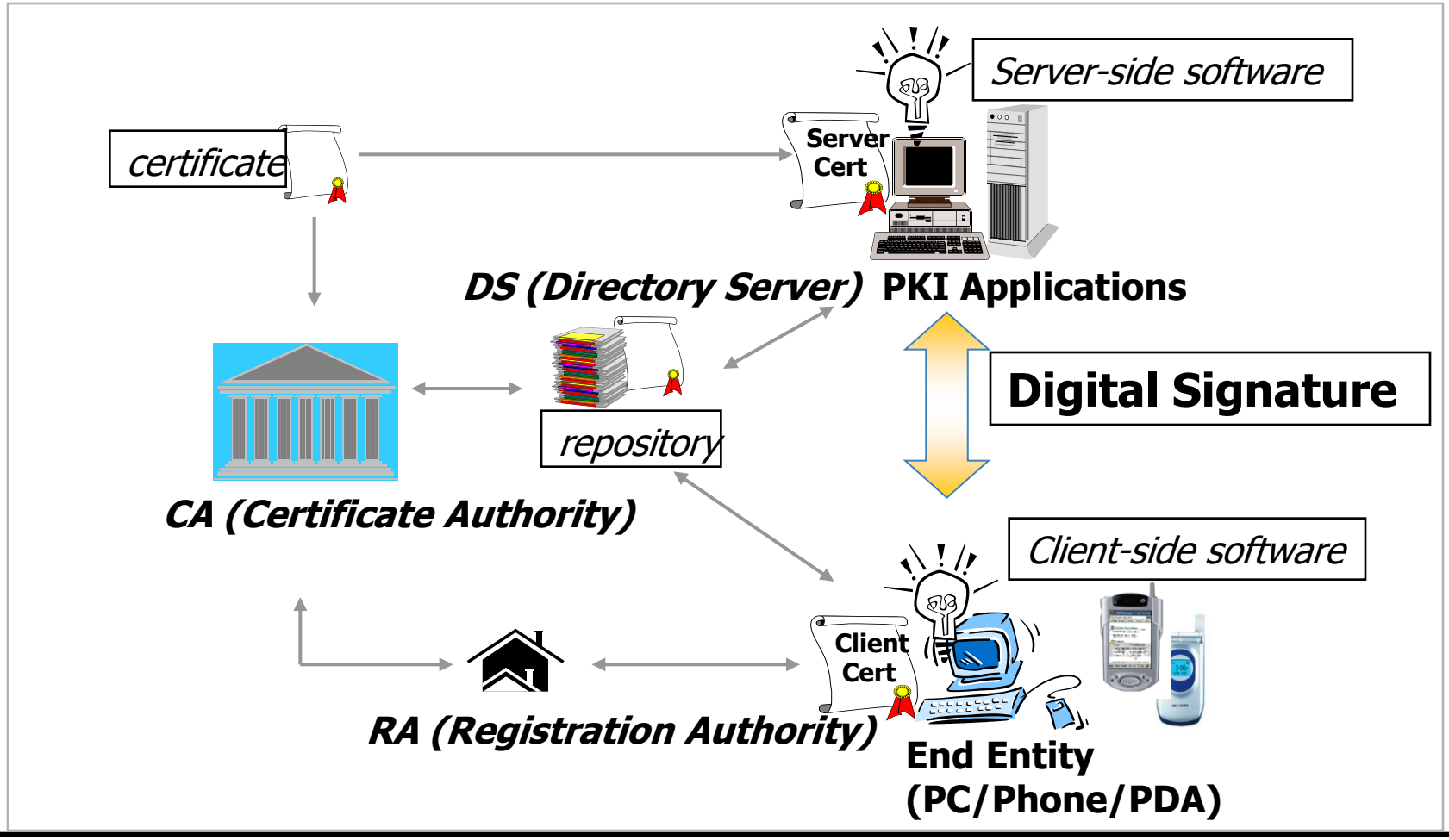


Need for Trust Third Part

- CA (Certificate Authority)

National PKI Framework

- Personnel, policy, procedures, components and facilities to bind user names to electronic keys so that applications can provide the desired security services.

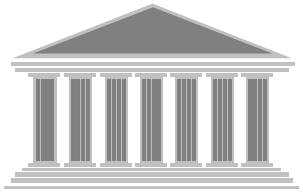


PKI Components

CA

Certificate Authority

- ❑ Issue or distribute the certificate for other CA, End Entity, RA.
- ❑ handle revocation request from the owner of certificate or RA.
- ❑ publish certificate and CRL to directory server
- ❑ issues the cross-certificate and manages



RA

Registration Authority

- ❑ identify the user and register the user information
- ❑ transmit certificate request to CA.
- ❑ search certificate and CRLs from directory server.
- ❑ request the certificate revocation

DS

Directory System

- ❑ store certificates (End Entity, RA, CA) and CRLs
- ❑ support LDAP (Lightweight Directory Access Protocol)

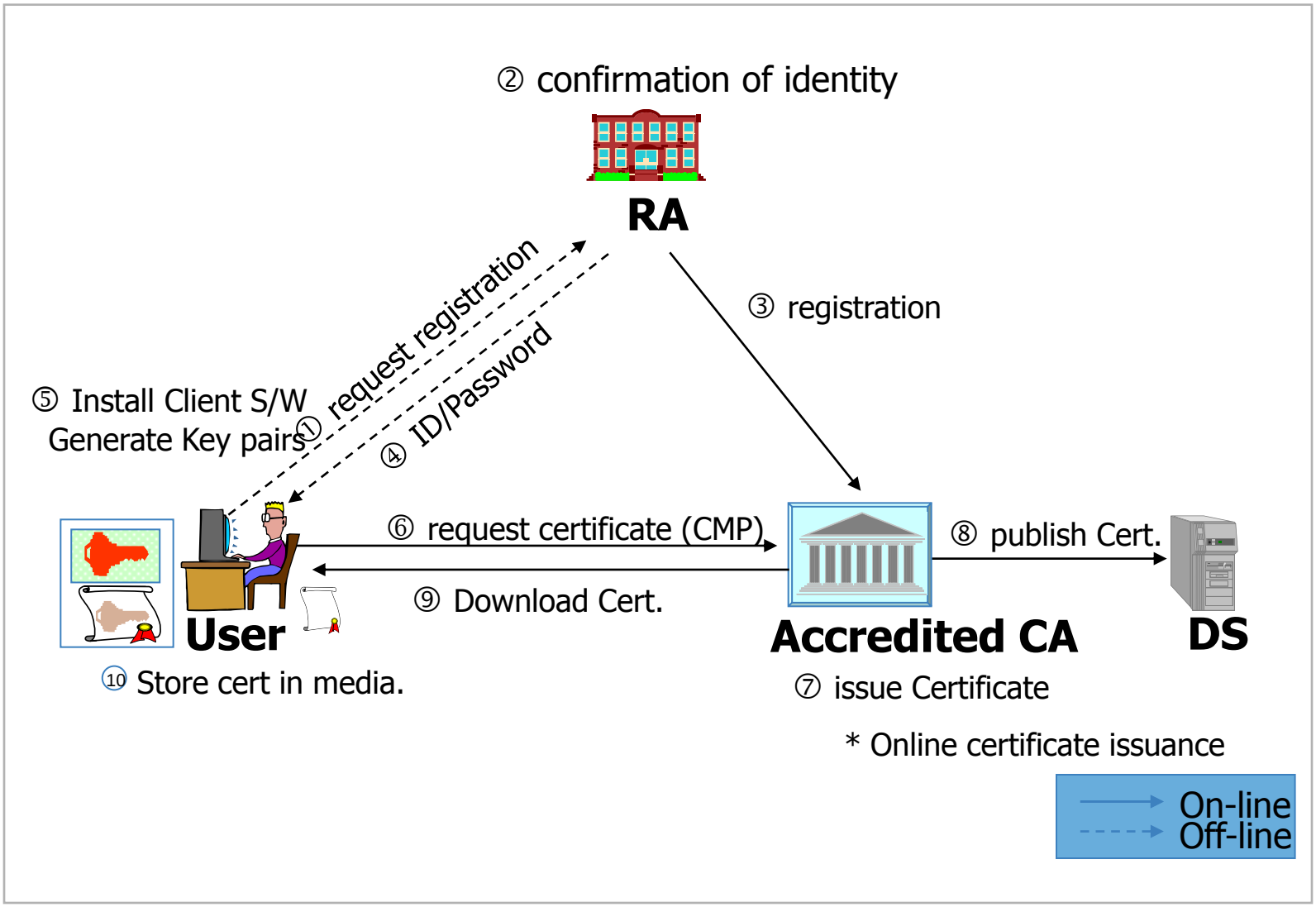
EE

End Entity

- ❑ Manage the certificate with certificate management software published by CA.
- ❑ Create digital signature and verify that.

NAISS

Process to issue certificates



I. PKI and Digital signature

2. Digital signature

NAISS

Need of Digital Signature

On the Internet, Nobody knows you're a dog

"On the Internet, nobody knows you're a dog."

Definition

Digital Signature

Digital signature is an unique digital data; it is applied to a document keeping the unique information of the signer with the digital signature creation key and make it possible to verify the entity authentication of document and whether there was modifications or not

It is not an Electronic signature but a Digital signature

NAISS

Comparison

	Electronic Signature	Digital Signature
Concept	Electronic data as an identifier 	Digital signature using asymmetric encryption / decryption method 13598293948977765839 19293933923939239239 49294959935939993953 99943049384550490594 49395234898434857558
Problem	Reusable	Impossible to reuse

No forgery	Can't make a signed document without a private key
No modification	Can't modify the signed document without the private key
Entity Authentication	The private key holder is the maker of the document
No reuse	Can't substitute the digital signature of "A" document to "B"
Non-repudiation	Can't repudiate signing of the private key holder

•Encryption/Decryption Type : RSA, DSS(Digital Signature Standard), ESIGN, Schnorr, KCDSA

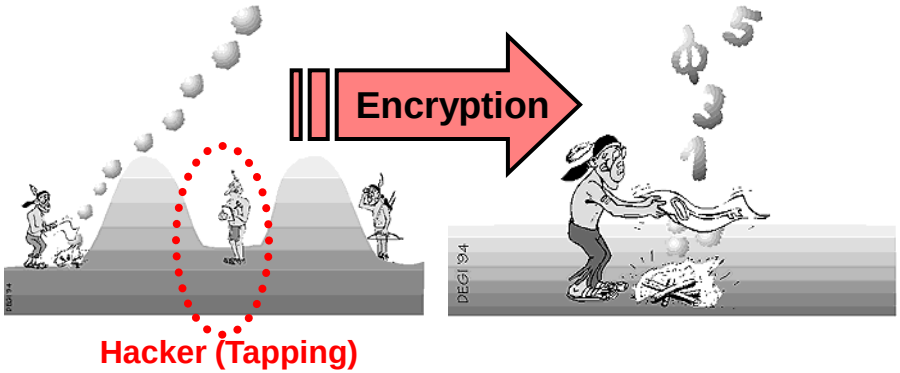
Feature of electronic document

ITEM	Paper document	Electronic document
Media	Paper	Digital media
Delivery	Mail, hand over	Network transmission
Safety of contents	Difficult to make forgery document or to modify Identification possible from physical characteristics of paper	Easy to make forgery document or modification Impossible to acknowledge forgery
Entity Authentication	Handwriting signature, Seal	Digital Signature

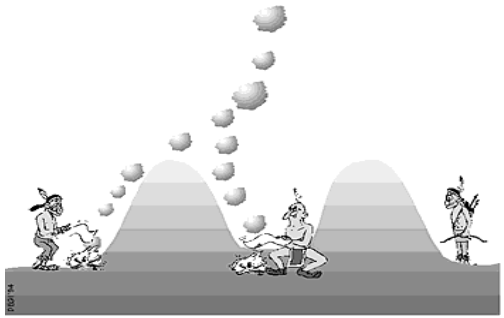
NAISS

Functions of Digital Signature

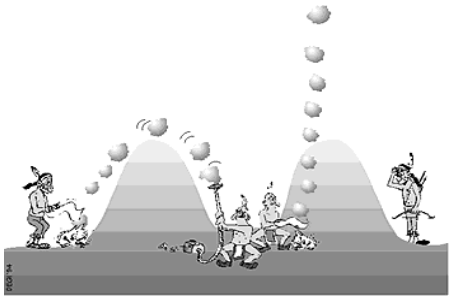
Confidentiality



Integrity

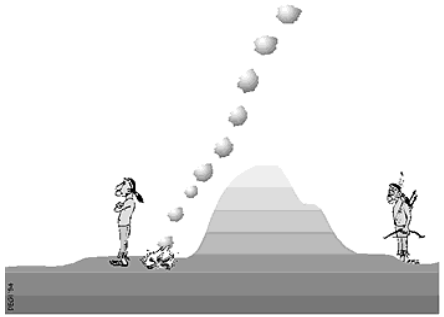


Source *Authentication*



Entity Authentication

Non-Repudiation

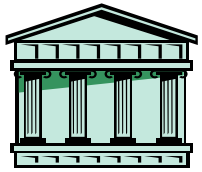


※ *Pictures are taken from the CryptMail User's Guide, Copyright (C) 1994 Utimaco Belgium, with the kind permission of Kurt Schoenmaekers, Managing Director.*

Authentication Process using Licensed certificate

Public key of "A" Public key of "B"

Licensed CA



2.Verify entity (face to face) and issue certificate

1.Certificate request

4.CA certificate and ceased list request

5.Certificate validation list transmission

6.Check validity
7.Certificate verification
8.Digital signature verification

Need of Licensed CA:

Verify public key of each one guarantee the effectiveness

User A

3.Digital signature creation and transmission
(Electronic document + Digital signature + Certificate)

User B

Private key of "A"

Private key of "B"

II. Large-Value Payment System in Korea (BOK-Wire)

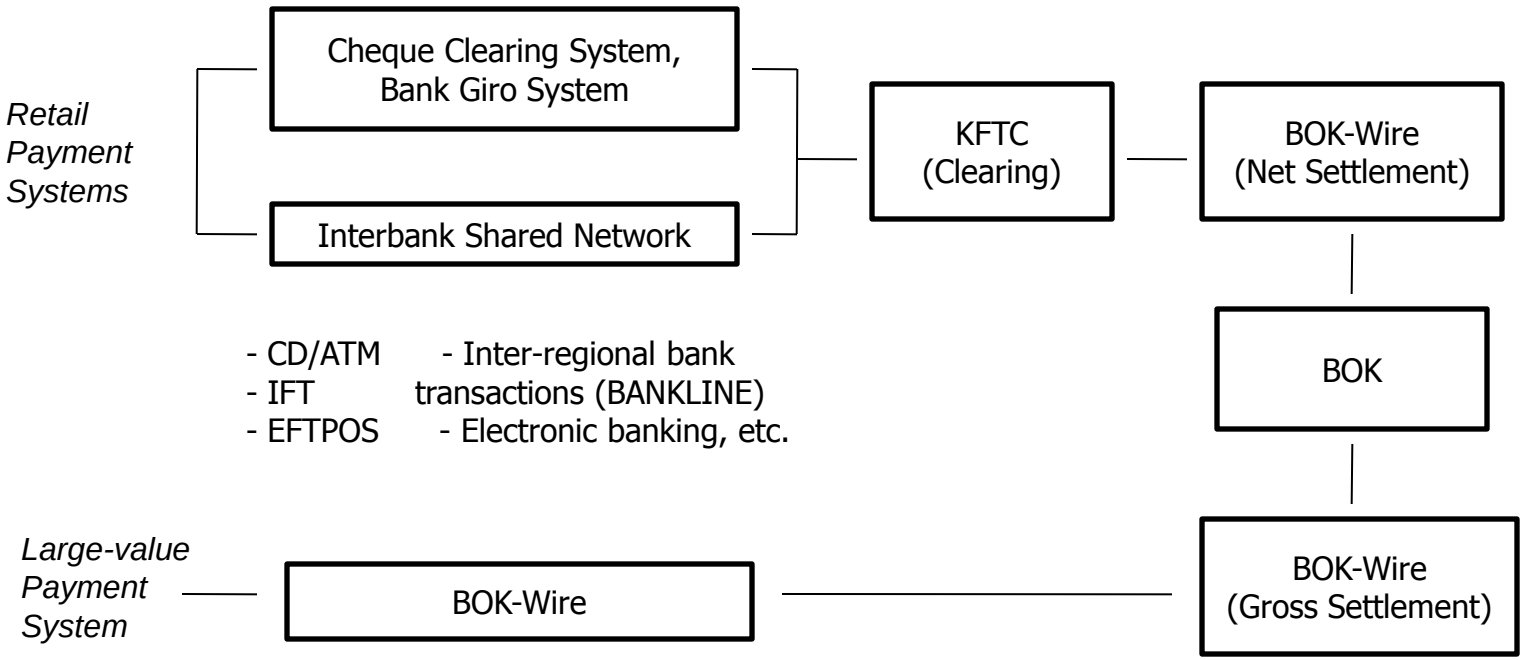
1. Outline

BOK-Wire

- The only RTGS System for large-value funds transfers between financial institutions in Korea
- Solely owned & Operated by The bank of Korea since December 1994
- Guarantees settlement finality for individual funds transfer requests by adopting the method of real-time gross settlement

1. Outline

Chart 1: Structure of Interbank Settlement Systems in Korea



2. Main Functions of BOK-Wire

Main Functions

- Domestic Currency Funds Transfers
- Foreign Currency Funds Transfers
- Net Settlement of Retail Payments
- BOK Loans
- Government & Public Bonds Issuance & Redemption
- Government Treasury Funds Transfers

NAISS

2. Main Functions of BOK-Wire

Domestic Currency Funds Transfers

- The General Settlement of Domestic Currency Funds Transfer Service

  - The transfer of funds between participants and their head office and local branches across current account with the Payment Systems Dept. of BOK or its regional headquarters

- Call Transaction Settlement

  - The supply and repayment of call funds across participants' current accounts with the BOK so as to adjust temporary excesses and shortages of funds

2. Main Functions of BOK-Wire

Domestic Currency Funds Transfers

- Recipient-Specific Funds Transfer

  - Companies and individuals are able to transfer large-value funds to their customers accounts through BOK-Wire participants

- Delivery versus Payment (DVP) Settlement of Funds

  - Since November 1999, the BOK has linked BOK-Wire with the Book-entry system of KSD for settling the funds for securities transaction

NAISS

2. Main Functions of BOK-Wire

Foreign Currency Funds Transfers

- Because of the duty related reserve requirements on foreign currency deposit, the required reserves are deposited in US Dollar or Japanese Yen at the BOK foreign currency accounts

- US Dollar and Japanese Yen transfers are available between participants' foreign currency accounts with BOK

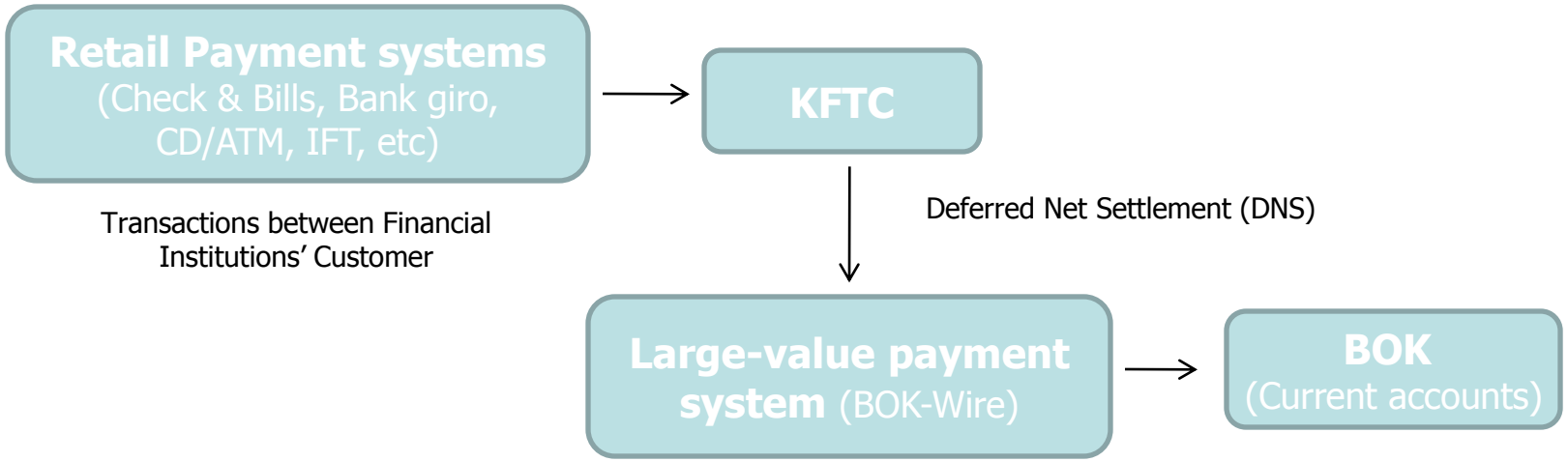
  - In this way reserve account balances are conveniently adjusted between banks with excess reserves and banks with insufficient reserves

2. Main Functions of BOK-Wire

Net Settlement of Retail Payments

- BOK-Wire enables participants to settle net positions of retail payments such as Check & Bills, bank giro and CD/ATM transactions

- Net obligations of retail payments are settled at two designated times, 11:00 and 14:00, depending on the type of payment



2. Main Functions of BOK-Wire

BOK Loans

- Bok-Wire is used for dealing with file transfers and funds settlement related to the BOK Loans System

Government & Public Bonds Issuance & Redemption

- Bok-Wire provides participants with settlement services related to issue, transfer, repurchase and redemption of government bonds and BOK Monetary Stabilization Bonds

Government Treasury Funds Transfers

- Treasury payment system carries out the collection of tax revenues by concentrating at the BOK the Treasury funds received by Treasury agencies nationwide

NAISS

3. Intraday Liquidity Management

Intraday Liquidity Management

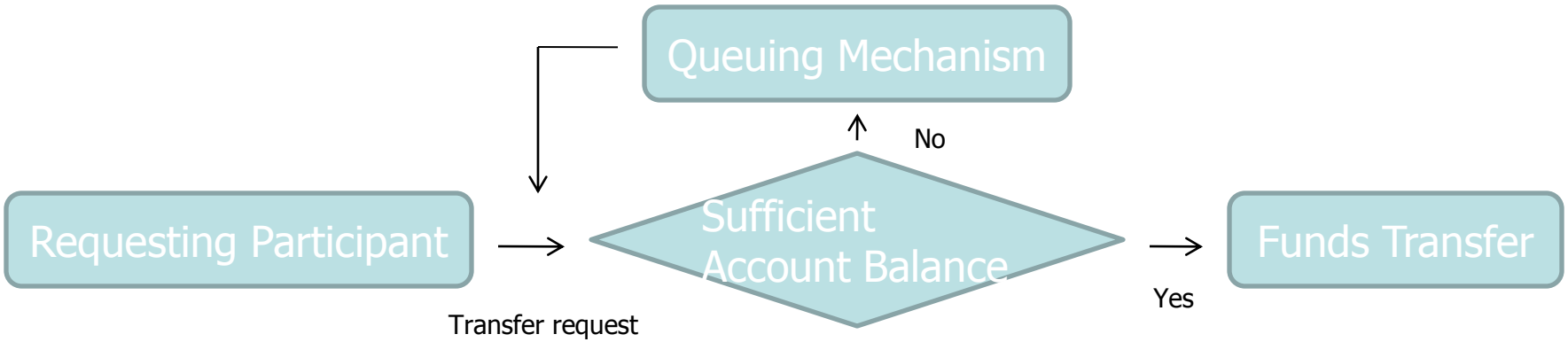
- Queuing Arrangements
- Designated – Time transaction System
- Advance Funds Transfer Arrangements
- Half-day Call Transaction
- Intraday Overdrafts

NAISS

3. Intraday Liquidity Management

Queuing Arrangements

- BOK-Wire adopts a Queuing Mechanism when participants are short of the required current account balance
- Typically such a system holds the payment orders in a queue until the necessary funds are credited.
- By-pass FIFO and Optimization routines have been introduced to improve system liquidity settlement efficiency



3. Intraday Liquidity Management

Designated–Time Transaction System

- BOK-Wire designates the time to process net settlement in Check & Bills, Bank giro, and IFT at the order of KFTC, redemption of Call Funds at maturity, and collection of Treasury Funds from Financial Institutions

- Integrated processing of large-value transactions at one point in time heightens the efficiency of financial institutions' liquidity management and the convenience of settlement business

NAISS

3. Intraday Liquidity Management

Designated-Time Transaction System

	Classification	Time
Morning net settlement	Bank giro, CD/ATM, Interbank Funds Transfer, Electronic Funds Transfer, CMS, BANK LINE, Electronic Money, B2C, B2B, Electronic Banking, Check Clearing(in Seoul, Elec tronic Bill)	11:00
Afternoon net settlement	Check Clearing(excluding transactions settled at the morning net settlement time)	14:00
Withdrawal of Treasury funds		14:00
Delivery of call loans	Morning half-day call	11:00
	Afternoon half-day call	14:00
Repayment of call money	Morning half-day call	14:00
	Afternoon half-day call	16:00
	One-day or longer period call	11:00
Execution of Advance funds transfer arrangement	Morning Advance funds transfer arrangement	11:00
	Afternoon Advance funds transfer arrangement	14:00
Deposits in foreign currency		16:00

3. Intraday Liquidity Management

Advance Funds Transfer Arrangement

- The Advance Funds Transfer Arrangement System is designed to heighten the counterparties' convenience by making advance funds transfer arrangement for a designated time to cover the funds shortage in net settlement of retail payments

- The arrangement should be filed between the time that the BOK receives net settlement requests from KFTC and the designated time(11:00, 14:00)

NAISS

3. Intraday Liquidity Management

Half-day Call Transaction

- Half-day Call Transaction System is designed to facilitate financial institutions' coverage of intraday funds' shortage for Net Settlement of retail payments

- Half-day Call Transactions are of the two type; morning and afternoon session.

  - Half-day Call Transaction Funds are automatically redeemed at maturity through BOK-Wire

NAISS

3. Intraday Liquidity Management

Intraday Overdrafts

- Daily current account loan is an instrument that facilitates the smooth operation of the RTGS
- When the current account balance of a participant falls short of the amount of the funds transfer order, the system immediately supports an automatic loan within the preset credit limit to allow funds settlement to operate continuously during business hours
- Government bonds, government guaranteed bonds, monetary stabilization bonds (MSB) are held as a collateral for the daily current account loan
- When the loan is not repaid before the deadline, it is converted into Liquidity Adjustment Loan, carrying a relatively high interest rate

NAISS

4. Management

Participation

- Access conditions
  - Having a current account with the BOK
  - Forecast number usage : more than 20 monthly
  - Management guidance ratios (e.g. BIS Capital Adequacy Ratios)

- As of the end of March 2009, a total of 128 institutions participated in BOK-Wire of which 54 were banks and 74 were non banks

Classification	Domestic Bank	Foreign Bank	Securities	Insurance	Etc	Total
Number	18	36	53	9	12	128

5. Next Generation of BOK-Wire

- Hybrid Settlement System
  - In order to enhance the liquidity settlement efficiency, BOK will combine RTGS with Bilateral and Multilateral Net Settlement

- Server to Server Interface
  - from Terminal vs Server to Server vs Server

- Realtime Monitoring system
  - To enhance Intraday liquidity management

III. Retail Payment System in Korea

(KFTC)

1. Outline

KFTC

- The only ACH (Automatic Clearing House) in Korea
- The Korea Financial Telecommunications and Clearing Institute (KFTC) is a non-profit organization on a joint-ownership basis by member banks including the Banks of Korea since 1986.
- KFTC is the operator of all retail payment systems in Korea and operates a SWIFT (Society for Worldwide Interbanks Financial Telecommunication) Access Point.
- KFTC has three classes of membership ; general, associate and special. (12 general members, 12 associate members and 14 special members as of 2001)

NAISS

2. Check Clearing System

- The Check Clearing System is owned and operated by KFTC.

- Checks are automatically sorted and have an MICR (magnetic ink character recognition and delivered to the clearing house for overnight by 1:00 on day T+1.

- In the Clearing House, checks are cleared by online transmission of digital information only. (without physical delivery)

- Following the KFTC's notification, the Bank of Korea settles at the designated time 14:30 (13:00 on Saturday) on day T+1.

- Risk management
  - In order to contain systemic risk, the Check Clearing System has collateral arrangements to provide government Bonds or BOK MSBs to BOK. (30% of daily average obligation)

NAISS

3. Banks Giro System

- The Banks Giro System was introduced in 1977 and also owned / operated by KFTC.

- The Banks Giro, still accounting for about 20% of all non-cash retail payments, is the most efficient solution for companies' paying and collecting large volume of recurring bills.

- In case of paper-based credit transfer, giro bills are deliverd to KFTC on day T and settled at BOK on day T+2.

- Risk management
  - Same as Check Clearing System

4. Interbank Funds Transfer (IFT) System

- This system enables a customer visiting a bank branch to transfer funds to a payee holding an account at any bank across the nation on a real time basis.

- Interbank settlement is finalized at 11:30 on the next business day by BOK.

- Risk management
  - Similar collateral requirement is set up under the control of BOK.

NAISS

5. Interbank CD/ATM System

- The interbank CD/ATM System, launched in 1988, is owned and operated by KFTC.
- The recent increase of unstaffed bank branches has greatly influenced the installations of off-premise CDs and ATMs.
- The number of CDs and ATMs in Korea was 1.02 machines per 1,000 habitants as of 2000.
- The ATM owner sends the information transmitted by card holder to the card issuer through KFTC's switching computer.
- Introduction funds settlement in this system is completed at 11:30 on the next business day through the banks' account at BOK.

6. Electronic Funds Transfer at the Point of Sale System

- This system was organized as an interbank network in 1996 and owned and operated by KFTC.
- The EFTPOS System enables debit card holders to purchase goods and services from any affiliated retailers by providing them with electronic access at the point – of – sale to their banks accounts.
- The interbank net positions are calculated by KFTC and are then settled across the banks' accounts held with BOK at 11:30 on next day of trade date.
- After interbank settlement has been completed, the bank transfers the relevant funds to the retailer's account on the same day.

NAISS

7. Electronic Banking System

- The Electronic Banking System was organized as an interbank shared network in 2001 and owned / operated by KFTC.
- The users of Internet Banking and mobile banking are rapidly increasing due to more than 90% penetration rate nationwide.
- Any Internet Banking user must obtain a digital certificate from CA through the internet.
- Internet transactions made with digital certificates have legal validity in Korea under the Digital Signature Law.
- BOK settles the interbank net positions for funds transfer done by 23:30 at 11:30 on the day after the trade date.

NAISS