

Information Security

Eom, Hyeonsang (엄현상)

Department of Computer Science & Engineering
Seoul National University (SNU)

2022.5.17

❖ 서울대학교 우리은행 교육과정 핀테크 산업 응용 2차시 강의 파트 II



Motivating Example: Secure Information Transfer



User A



User B

❖ How Can User A Send Information Securely to User B?

- What Does This Mean?

Outline

❖ Security Techniques

- Basic Security Concepts
- Cryptography Basics
- Digital Signature
- Digital Envelope
- Certificate
- Illustration: Public Key Infrastructure

❖ Security – Convergent Network World

❖ Summary

Basic Security Concepts

- ❖ **Identification (against All Entities)**
 - Process of Recognizing a Particular Individual Using Presented Information
- ❖ **Authentication (against a Previously Identified Entity)**
 - Process of Verifying Certain Information
- ❖ **Authorization**
 - Process of Determining What You Are Allowed to Do
- ❖ **Integrity**
 - Process of Ensuring That Information Is Unchanged
- ❖ **Confidentiality**
 - Keeping Information Secret
- ❖ **Non-Repudiation**
 - Not Being Able to Deny Something

Cryptography Basics

❖ Definition

- Science of Applying Mathematics to Increase Security

❖ Symmetric Cryptographic Algorithms

- Taking Clear Text as Input Outputting the Cipher Text Using a Symmetric Key, and Reversing This Process
 - DES (Data Encryption Standard)
 - 3-DES
 - RC2, RC5, RC6
 - Rijndael(or AES, Advanced Encryption Standard)

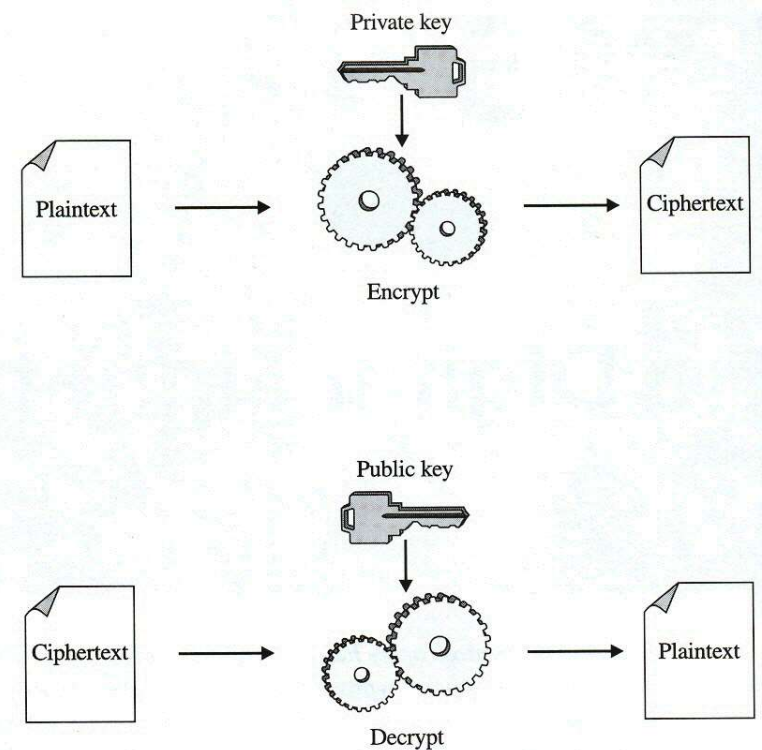
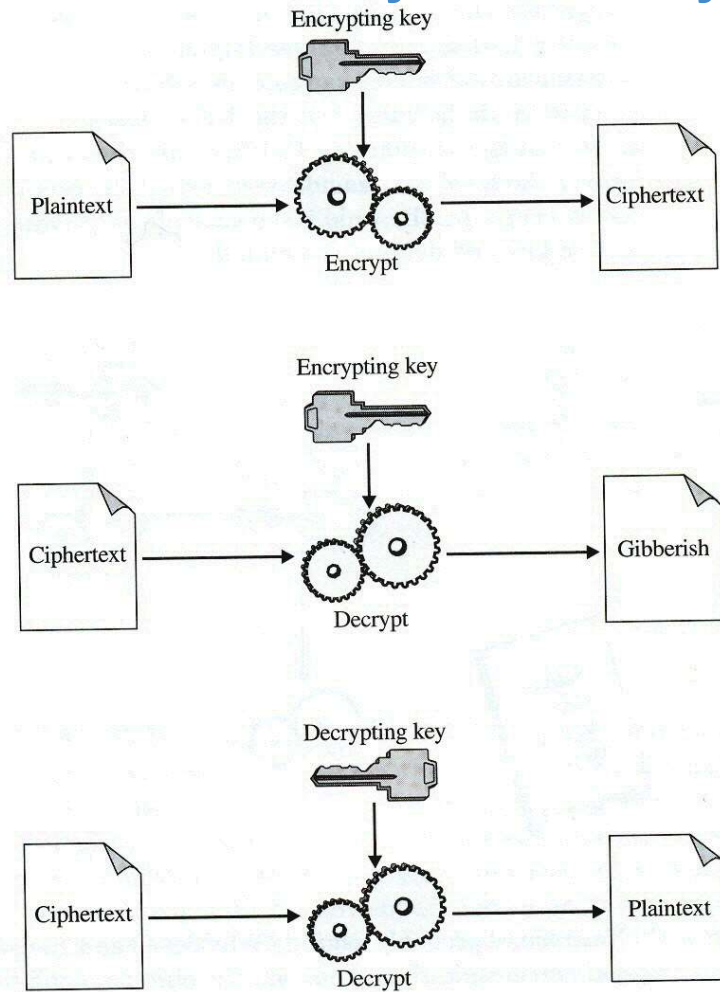
❖ Asymmetric Cryptographic Algorithms

- Taking Clear Text as Input Outputting the Cipher Text Using a Public/Private Key, and Reversing this Process Using the Matching Private/Public (Respectively) Key
 - DH (Diffie-Hellman)
 - RSA (Rivest, Shamir, and Adleman at MIT)
 - ECC (Elliptic Curve Cryptography)

PKI (Public Key Infrastructure): the Public/Private Key–Based Encryption Framework That Permits Deploying Security Services

Cryptography Basics (Cont'd)

❖ Illustrations: Asymmetric Cryptography



Cryptography Basics (Cont'd)

❖ Symmetric vs Asymmetric Cryptographic Algorithms

- Advantages of Asymmetric Algorithms
 - Superior key management and scaling
 - Unnecessary prior relationship
 - Private-key-holder only operations (as a basis for digital signatures and non-repudiation)
- Disadvantages of Asymmetric Algorithms
 - Possibly 10 to 100 times slower execution
 - Expansion of the ciphertext

Cryptography Basics (Cont'd)

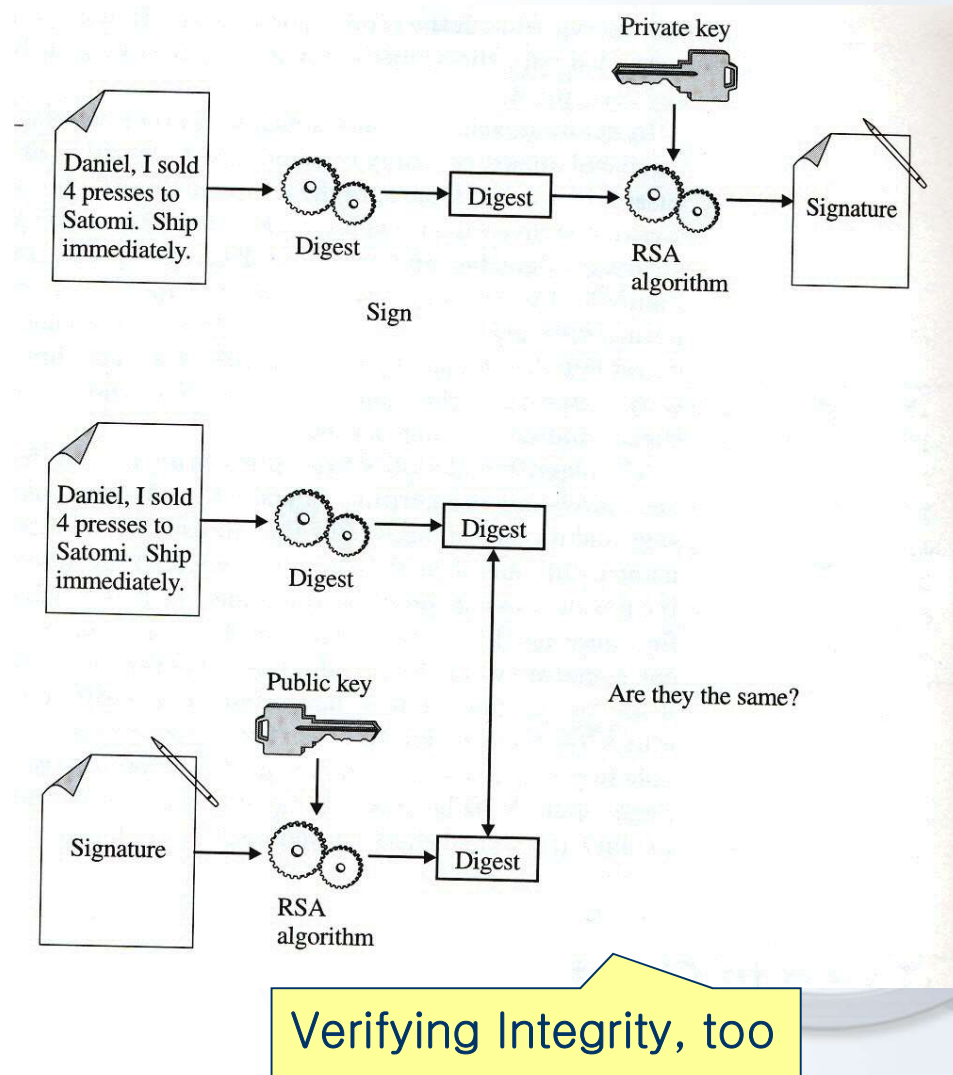
❖ Hash Algorithms

- Definition
 - Taking a chunk of data and compressing it into a digest (or fingerprint) of the data
- Examples
 - MD2 (128-bit digest; best for 8-bit processors)
 - MD5 (128-bit digest; best for 32-bit processors)
 - SHA-1 (160-bit digest; best for high-end processors)
- Properties
 - No backward recovery
 - No information about the initial clear text
 - No backward creation/discovery

Digital Signature

❖ Data Encrypted with a Private Key

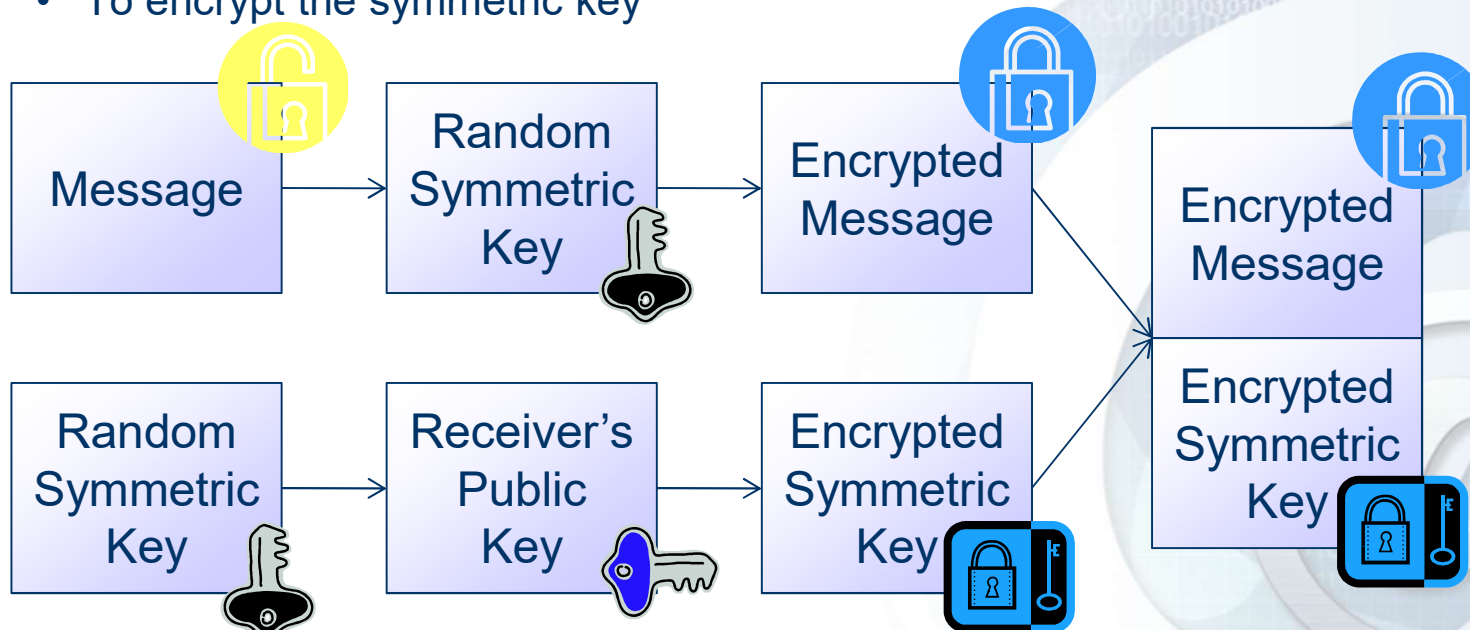
- Technique for Authentication and Non-Repudiation
 - If a public key properly decrypts data, then it must have been encrypted with the private key



Digital Envelope

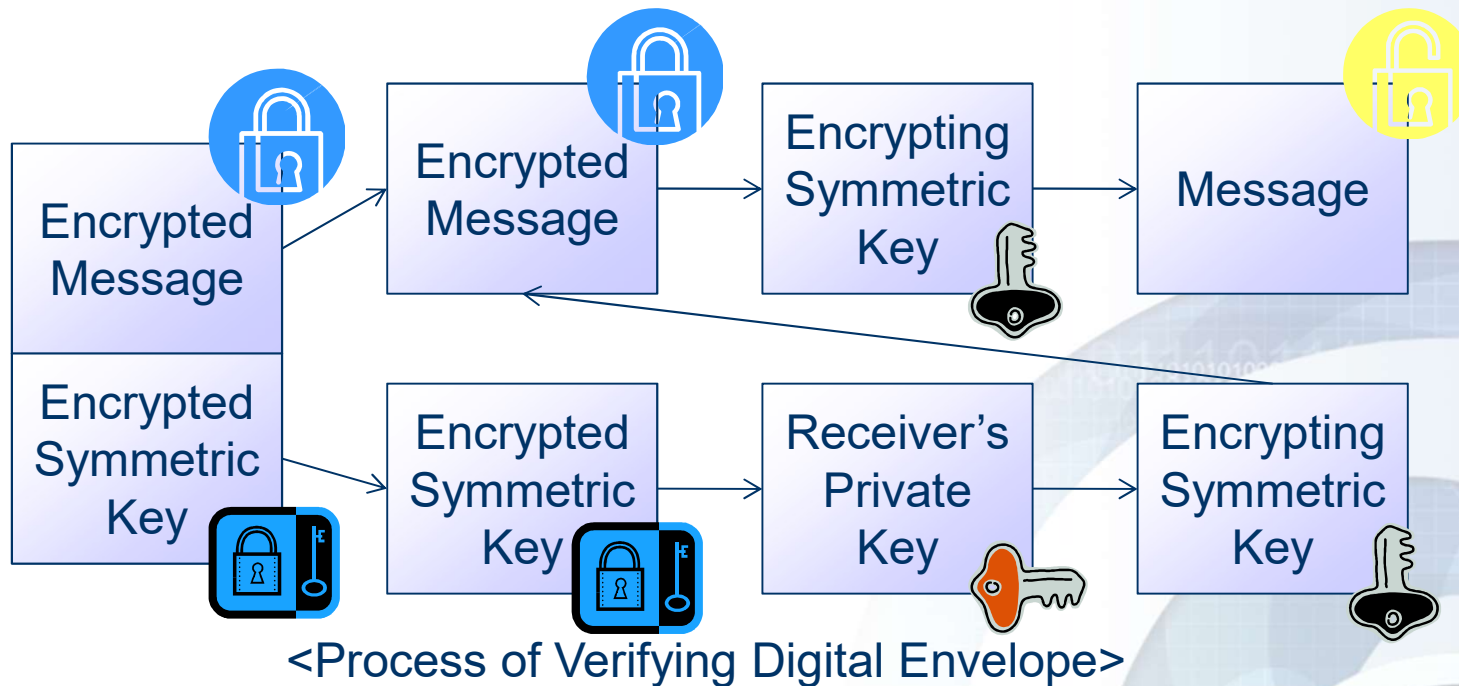
❖ Encryption That Uses Both Symmetric Key and Public Key

- Symmetric Key
 - To encrypt/decrypt messages
 - Symmetric algorithms: e.g., DES, 3-DES, RC4, etc.
- Public Key
 - To encrypt the symmetric key



<Process of Creating Digital Envelope>

Digital Envelope (Cont'd)

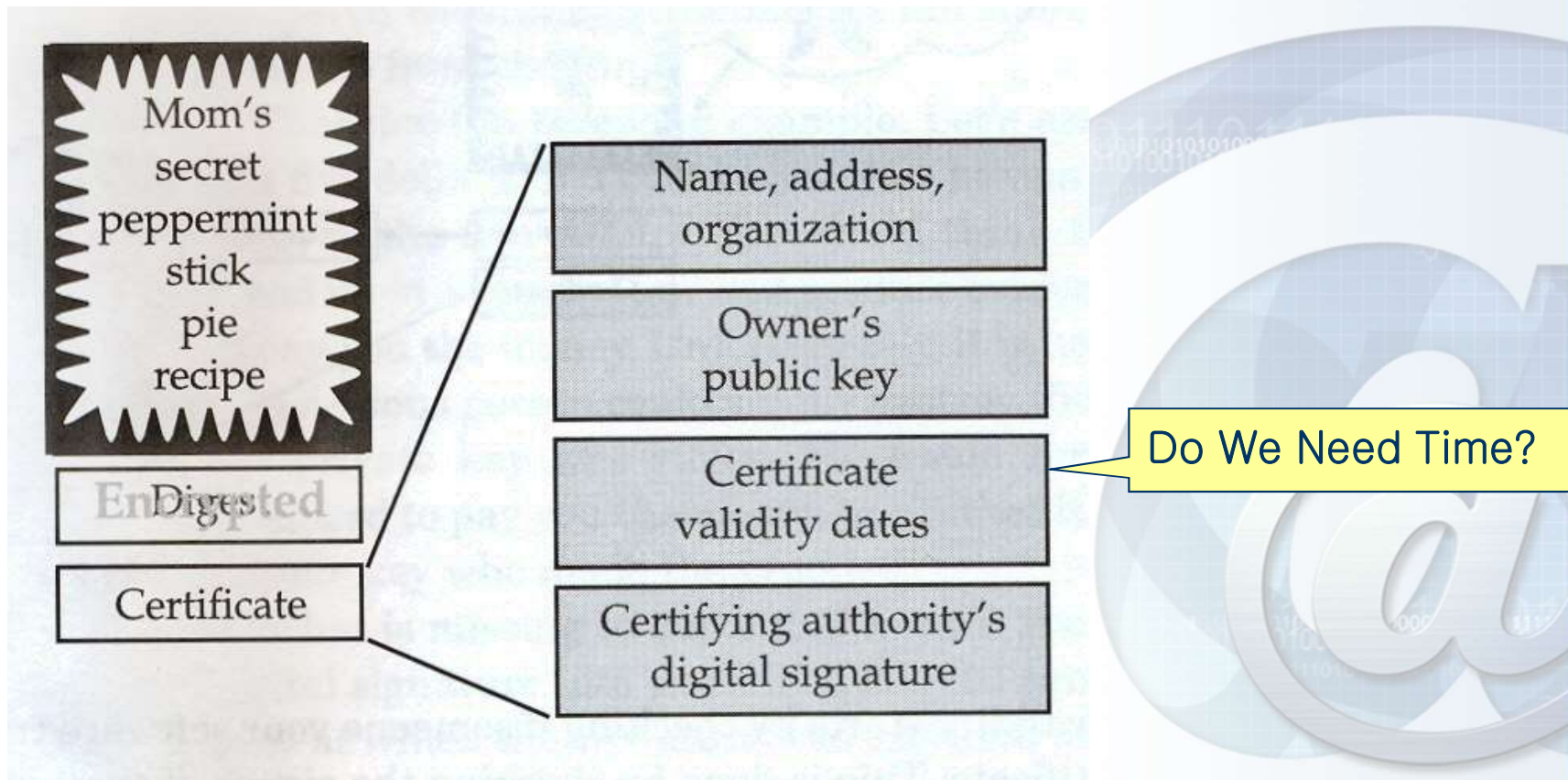


❖ Overcoming Performance Problem for Public Key Cryptosystems

- Efficiency Achieved Due to Protection of Only Key with Public Key

Certificate

❖ Notarized Association between the Particular User with the Particular Public Key



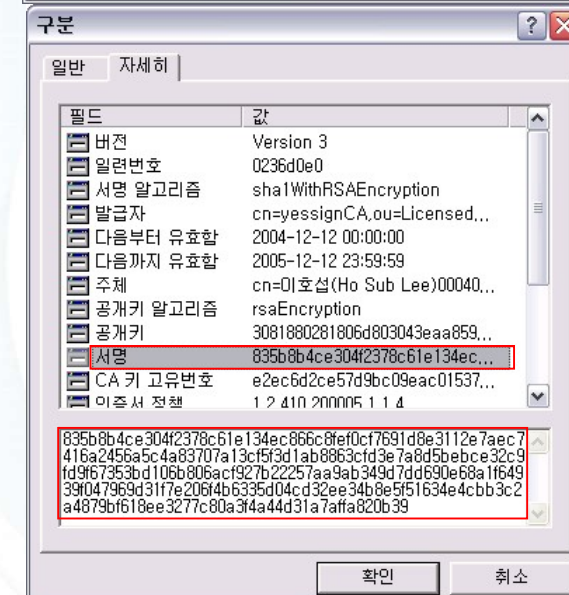
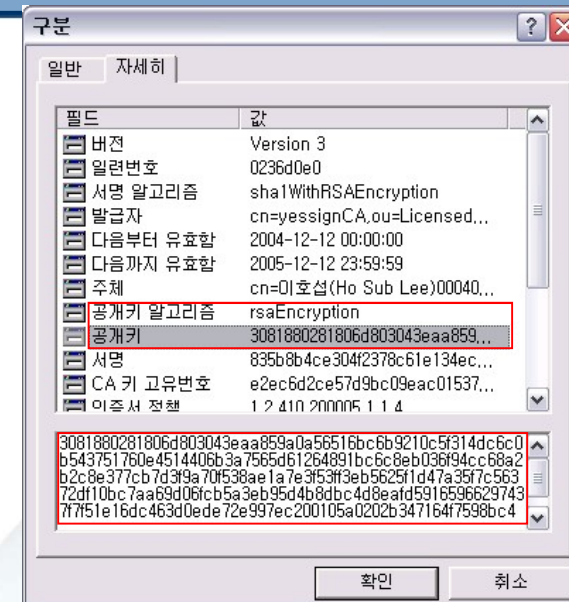
X.509 Certificate

❖ X.509 Specification

- Information Contained in a Certificate, and Its Format

❖ Components

- Version
 - Indicator of Version 1,2, or 3
- Serial Number
 - Unique Identifying Number for This Certificate
- Signature
 - Algorithm Identifier of the Digital Signature Algorithm
- Issuer
 - X.500 Name of the Issuing CA
- Validity
 - Start and Expiration Dates and Times of the Certificate
- Subject
 - X.500 Name of the Holder of the Private Key (Subscriber)
- Subject Public-Key Information
 - Value of the Public-Key for the Subject Together with an Identifier of the Algorithm with Which This Public-Key to Be Used



Security Holes in PKI

❖ Fabricated Identification Card

❖ Illegal Copy of Certificate

❖ Hacking Program

- E.g. Key Logger Program

- Hacker can get id/password, account no, security card no, and password for encrypting **private key**
- Hacker can disguise himself/herself as a user

The Main Reasons for These Security Holes Are Unsafe Storage, Operating System, and Character-Based Protection Mechanism.

👉 Security-Enabled Storage Medium, OS Security Patch, and Biometrics

Certificate Chain

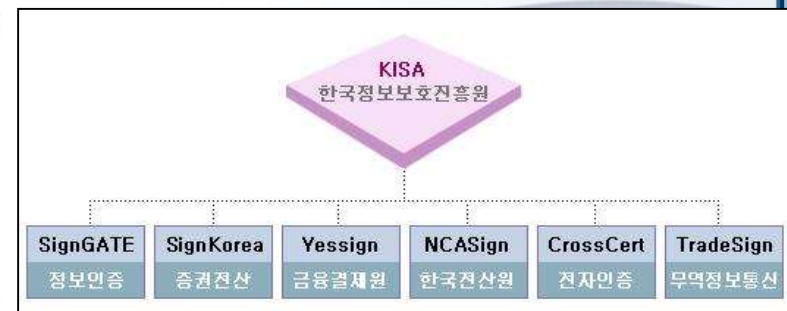
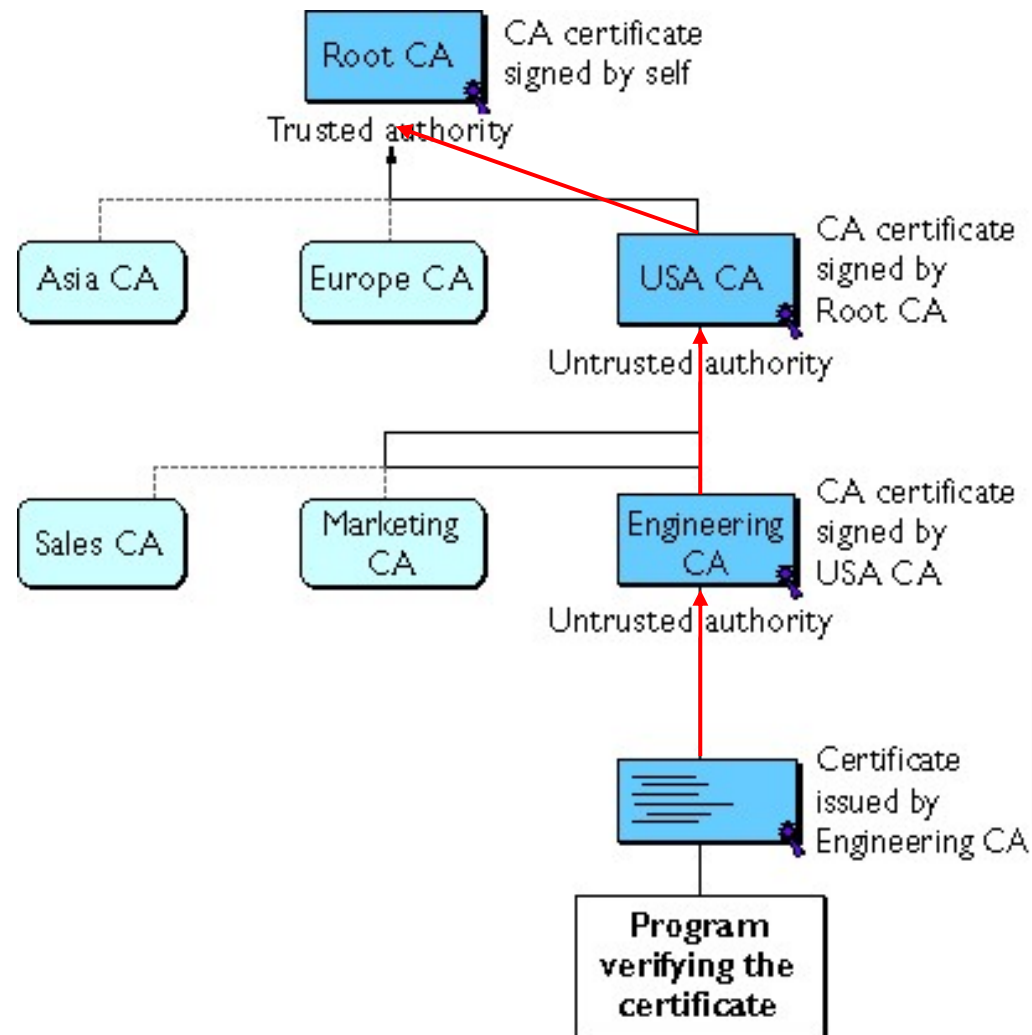
❖ X.509 Standard Model for Setting Up a Hierarchy of CAs

- In Large Organizations, It May Be Appropriate to Delegate the Responsibility for Issuing Certificates to Several Different Certificate Authorities

❖ Ordered List of Certificates Containing an End-User or Subscriber Certificate and Its Certificate Authority Certificates

- Each Certificate Is Followed by the Certificate of Its Issuer
- Each Certificate Contains the Name (DN) of That Certificate's Issuer
 - Same as the subject name of the next certificate in the chain
- Each Certificate Is Signed with the Private Key of Its Issuer
 - Signature verifiable with the public key in the issuer's certificate, which is the next certificate in the chain

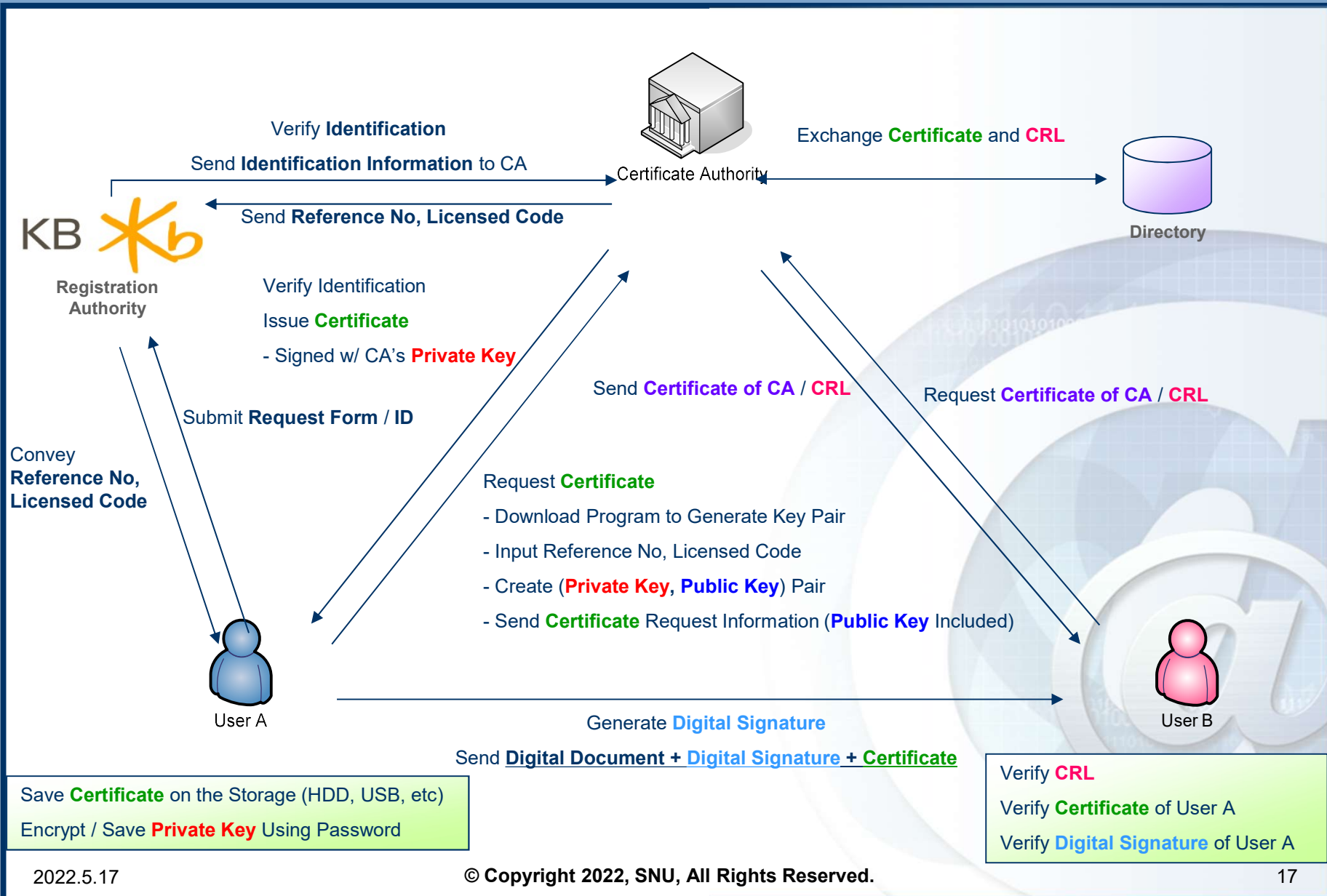
Certificate Chain Example



Korea

- Check Validity Period
- Verify That This Is Signed by Engineering CA
- Since Engineering CA Is Not Trusted, Check the Next Certificate

Illustration: Public Key Infrastructure

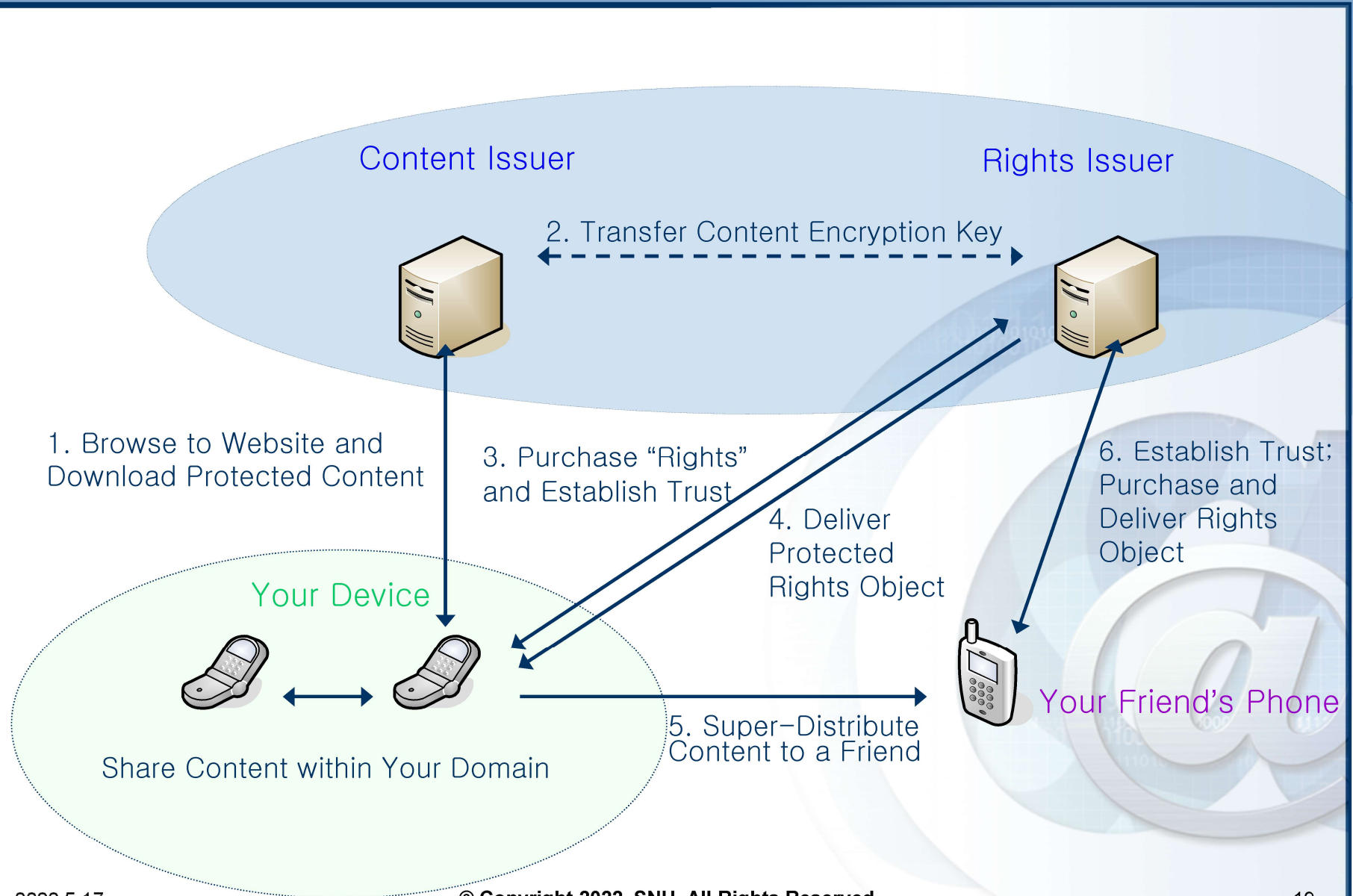


Applying DRM to Protect Content

❖ Distributing DRM Protected Content

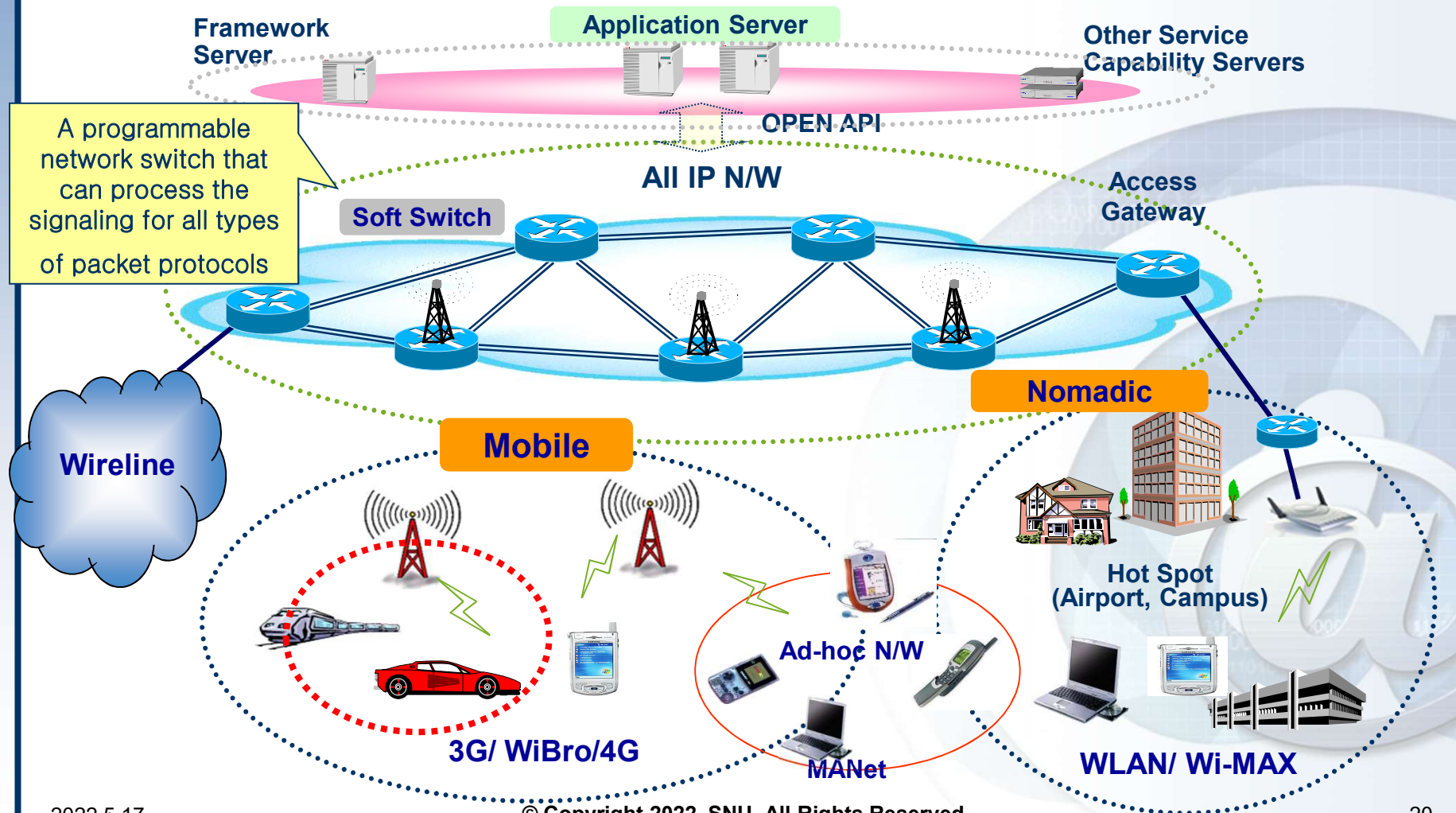
- Content Issuer's Encrypting the Content and Packaging in DRM Content Format
- Rights Issuer's Assigning Permissions and Constraints for Content
- User's Receiving Content and Rights
- User's Sending the Protected Content to a Friend with OMA DRM Enabled Devices
- Friend's Purchasing the Permission to Consume the Content

Example of OMA DRM Deployment



Security - Convergent Network World

Security (& Privacy) Issues Everywhere!



Summary

❖ Security Techniques

- Basic Security Concepts
 - Authentication
 - Integrity
 - Confidentiality
 - Non-Repudiation
- Cryptography Basics
 - Symmetric vs Asymmetric Cryptographic Algorithms
- Digital Signature
- Digital Envelope
- Certificate
- Illustration: Public Key Infrastructure

❖ Security – Convergent Network World

Security
Everywhere!

References

- [Burnett01] S. Burnett and S. Paine, *RSA Security's Official Guide to Cryptography*, Osborne/McGraw-Hill, March 2001
- [Nas01] A. Nash, et al., *PKI: Implementing and Managing E-Security*, Osborne/McGraw-Hill, March 2001
- [OMA] Open Mobile Alliance, www.openmobilealliance.org

Thank You !

Eom, Hyeonsang (엄현상)

hseom@snu.ac.kr

Department of Computer Science & Engineering
Seoul National University

