NetSec-KR

DID에 대한 오해와 진실

고려대학교 정보보호대학원 교수
국방 RMF 연구센터(AR²C) 센터장
고신뢰 보안운영체제 연구센터(CHAOS) 센터장

김 승 주 (Seungjoo Kim)

(Home) www.KimLab.net (Blog) www.Crypto.kr

고려대학교 정보보호학부 · 정보보호대학원
Korea University Division of Information Security
Graduate School of Information Security

DIDs : Decentralized IDentifiers

DIDs : Decentralized IDentifiers

- DIDs are a type of identifier that enables a **verifiable, decentralized digital identity**.
- A DID identifies any subject (e.g., a person, organization, thing, data model, abstract entity, etc.) that **the controller of the DID decides** that it identifies.
- These identifiers are designed to enable the controller of a DID to prove control over it and to be **implemented independently** of any centralized registry, identity provider, or certificate authority.

("Decentralized Identifiers (DIDs)", World Wide Web Consortium, 8 June 2020. Retrieved 22 June 2020.)

DIDs : Decentralized IDentifiers

- DIDs are URLs that associate a DID subject with a DID document allowing trustable interactions associated with that subject. Each DID document can express cryptographic material, verification methods, or service endpoints, which provide a set of mechanisms enabling a DID controller to prove control of the DID. Service endpoints enable trusted interactions associated with the DID subject. A DID document might contain semantics about the subject that it identifies. A DID document might contain the DID subject itself (e.g. a data model).

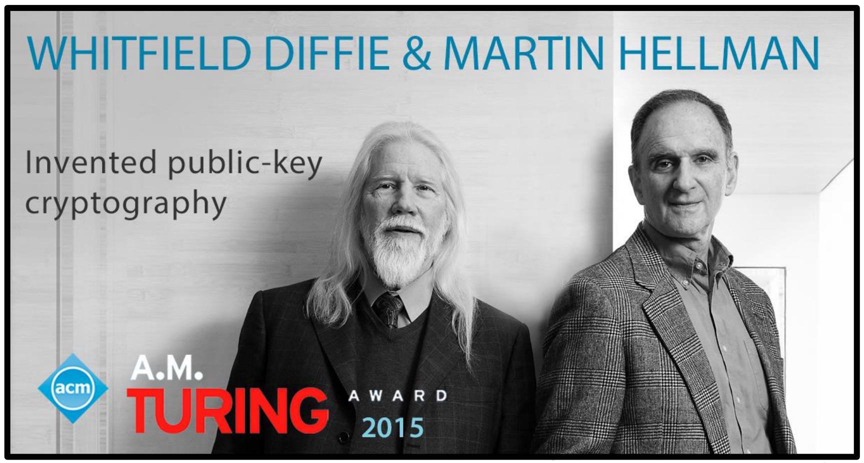
("Decentralized Identifiers (DIDs)", World Wide Web Consortium, 8 June 2020. Retrieved 22 June 2020.)

공개키암호와 전자서명 개념의 탄생 ('76)

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE



I. Introduction

We stand today on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create

mon occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.

Section III proposes two approaches to transmitting keying information over public (i.e., insecure) channels without compromising the security of the system. In a *public key cryptosystem* enciphering and deciphering are

A *public key cryptosystem* is a pair of families $\{E_K\}_{K \in \{K\}}$ and $\{D_K\}_{K \in \{K\}}$ of algorithms representing invertible transformations,

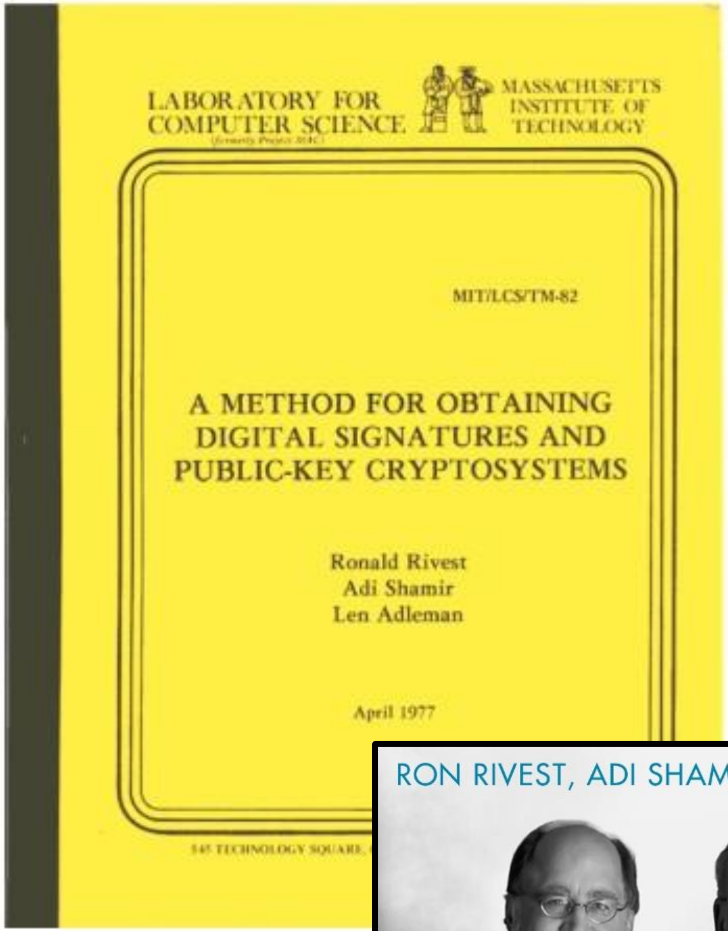
$$E_K:\{M\} \rightarrow \{M\} \qquad (2)$$

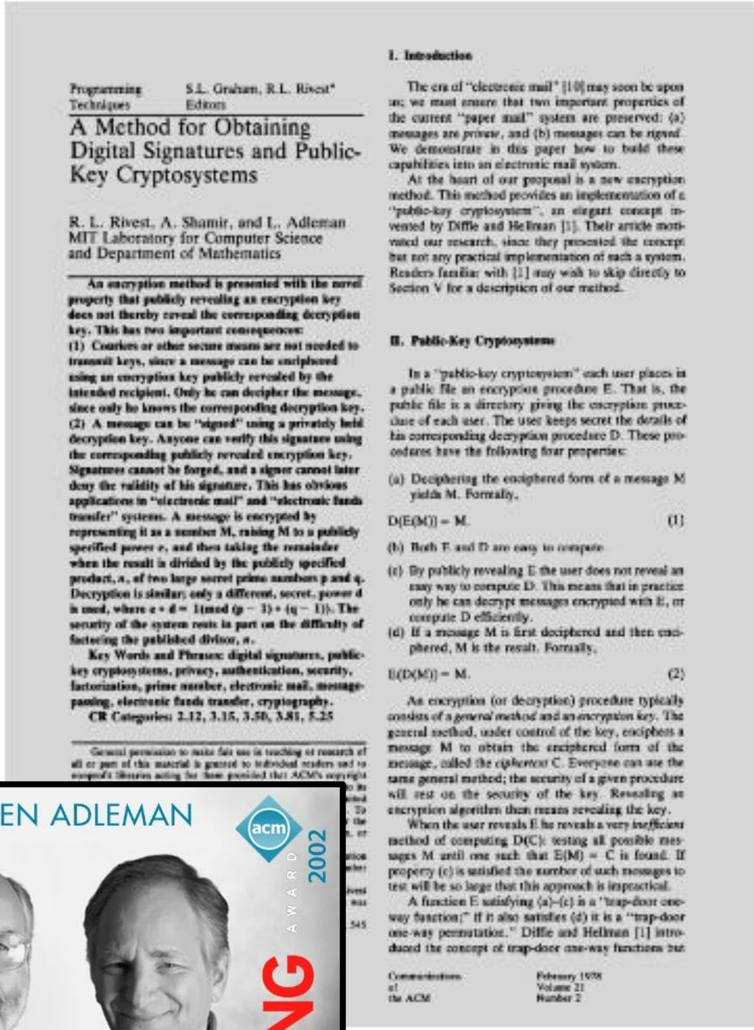
$$D_K:\{M\} \rightarrow \{M\} \qquad (3)$$

on a finite message space $\{M\}$, such that

1) for every $K \in \{K\}$, E_K is the inverse of D_K,
2) for every $K \in \{K\}$ and $M \in \{M\}$, the algorithms E_K and D_K are easy to compute,
3) for almost every $K \in \{K\}$, each easily computed algorithm equivalent to D_K is computationally infeasible to derive from E_K,
4) for every $K \in \{K\}$, it is feasible to compute inverse pairs E_K and D_K from K.

공개키암호와 전자서명 개념의 구현 ('78)





Programming Techniques — S.L. Graham, R.L. Rivest* Editors

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

R. L. Rivest, A. Shamir, and L. Adleman
MIT Laboratory for Computer Science and Department of Mathematics

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:
(1) Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key.
(2) A message can be "signed" using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged, and a signer cannot later deny the validity of his signature. This has obvious applications in "electronic mail" and "electronic funds transfer" systems. A message is encrypted by representing it as a number M, raising M to a publicly specified power e, and then taking the remainder when the result is divided by the publicly specified product, n, of two large secret prime numbers p and q. Decryption is similar; only a different, secret, power d is used, where $e \cdot d \equiv 1 \pmod{(p-1)\cdot(q-1)}$. The security of the system rests in part on the difficulty of factoring the published divisor, n.
Key Words and Phrases: digital signatures, public-key cryptosystems, privacy, authentication, security, factorization, prime number, electronic mail, message-passing, electronic funds transfer, cryptography.
CR Categories: 2.12, 3.15, 3.50, 3.81, 5.25

I. Introduction

The era of "electronic mail" [10] may soon be upon us; we must ensure that two important properties of the current "paper mail" system are preserved: (a) messages are *private*, and (b) messages can be *signed*. We demonstrate in this paper how to build these capabilities into an electronic mail system.

At the heart of our proposal is a new encryption method. This method provides an implementation of a "public-key cryptosystem", an elegant concept invented by Diffie and Hellman [1]. Their article motivated our research, since they presented the concept but not any practical implementation of such a system. Readers familiar with [1] may wish to skip directly to Section V for a description of our method.

II. Public-Key Cryptosystems

In a "public-key cryptosystem" each user places in a public file an encryption procedure E. That is, the public file is a directory giving the encryption procedure of each user. The user keeps secret the details of his corresponding decryption procedure D. These procedures have the following four properties:

(a) Deciphering the enciphered form of a message M yields M. Formally,

$$D(E(M)) = M. \quad (1)$$

(b) Both E and D are easy to compute.
(c) By publicly revealing E the user does not reveal an easy way to compute D. This means that in practice only he can decrypt messages encrypted with E, or compute D efficiently.
(d) If a message M is first deciphered and then enciphered, M is the result. Formally,

$$E(D(M)) = M. \quad (2)$$

An encryption (or decryption) procedure typically consists of a *general method* and an *encryption key*. The general method, under control of the key, enciphers a message M to obtain the enciphered form of the message, called the *ciphertext* C. Everyone can use the same general method; the security of a given procedure will rest on the security of the key. Revealing an encryption algorithm then means revealing the key.

When the user reveals E he reveals a very *inefficient* method of computing D(C): testing all possible messages M until one such that E(M) = C is found. If property (c) is satisfied the number of such messages to test will be so large that this approach is impractical.

A function E satisfying (a)-(c) is a "trap-door one-way function;" if it also satisfies (d) it is a "trap-door one-way permutation." Diffie and Hellman [1] introduced the concept of trap-door one-way functions but

Communications of the ACM — February 1978, Volume 21, Number 2

공개키암호와 전자서명 개념의 구현 ('78)

United States Patent [19]   [11] **4,405,829**

Rivest et al.   [45] **Sep. 20, 1983**

[54] **CRYPTOGRAPHIC COMMUNICATIONS SYSTEM AND METHOD**

[75] Inventors: **Ronald L. Rivest**, Belmont; **Adi Shamir**, Cambridge; **Leonard M. Adleman**, Arlington, all of Mass.

[73] Assignee: **Massachusetts Institute of Technology**, Cambridge, Mass.

[21] Appl. No.: **860,586**

[22] Filed: **Dec. 14, 1977**

[51] **Int. Cl.**[3] **H04K 1/00**; H04I 9/04
[52] **U.S. Cl.** **178/22.1**; 178/22.11
[58] **Field of Search** 178/22, 22.1, 22.11, 178/22.14, 22.15

[56] **References Cited**

U.S. PATENT DOCUMENTS

3,657,476 4/1972 Aiken 178/22

OTHER PUBLICATIONS

"New Directions in Cryptography", Diffie et al., *IEEE Transactions on Information Theory*, vol. IT–22, No. 6, Nov. 1976, pp. 644–654.
"Theory of Numbers" Stewart, MacMillan Co., 1952, pp. 133–135.
"Diffie et al., Multi–User Cryptographic Techniques", AFIPS. Conference Proceedings, vol. 45, pp. 109–112, Jun. 8, 1976.

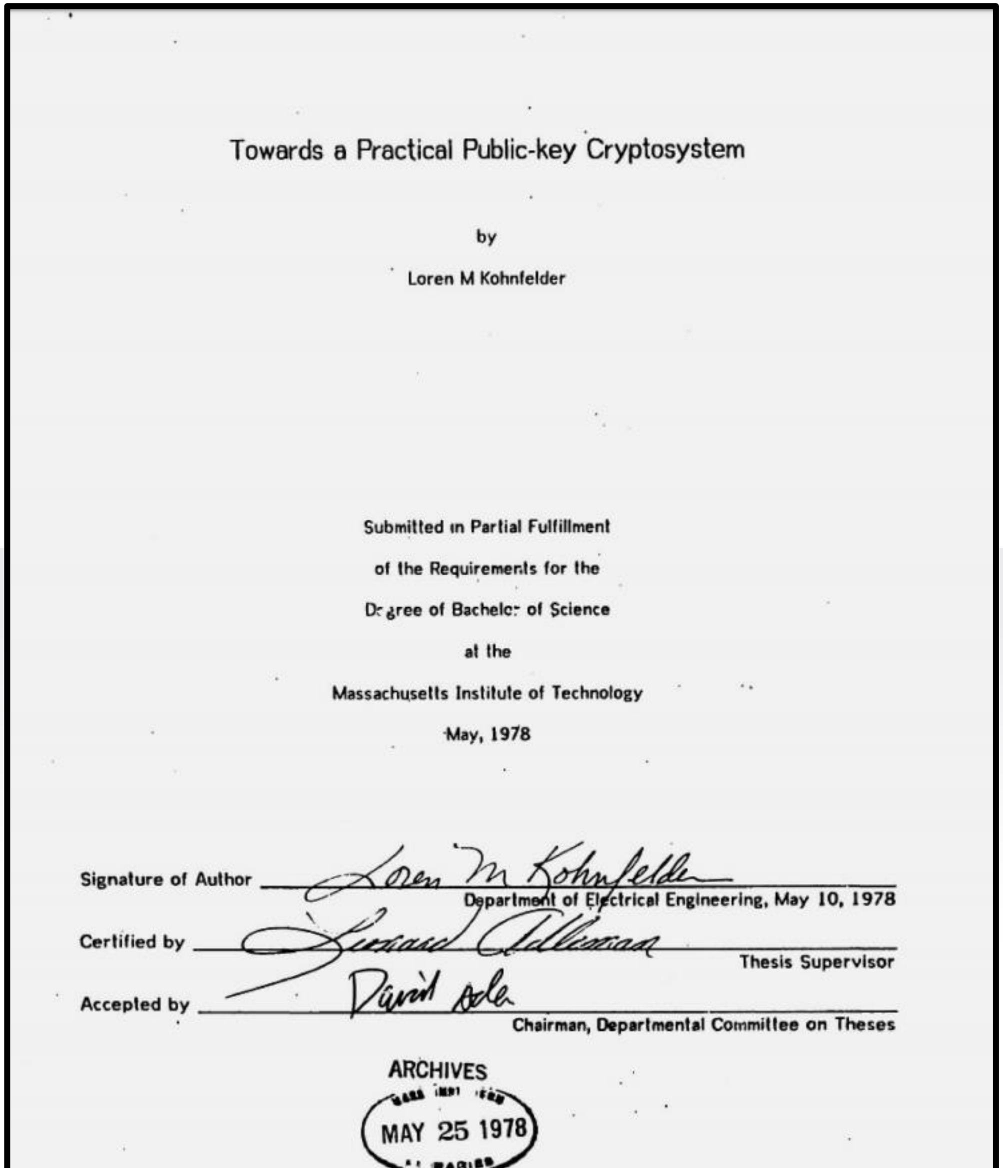
Primary Examiner—Sal Cangialosi
Attorney, Agent, or Firm—Arthur A. Smith, Jr.; Robert J. Horn, Jr.

[57] **ABSTRACT**

A cryptographic communications system and method. The system includes a communications channel coupled to at least one terminal having an encoding device and to at least one terminal having a decoding device. A message-to-be-transferred is enciphered to ciphertext at the encoding terminal by first encoding the message as a number M in a predetermined set, and then raising that number to a first predetermined power (associated with the intended receiver) and finally computing the remainder, or residue, C, when the exponentiated number is divided by the product of two predetermined prime numbers (associated with the intended receiver). The residue C is the ciphertext. The ciphertext is deciphered to the original message at the decoding terminal in a similar manner by raising the ciphertext to a second predetermined power (associated with the intended receiver), and then computing the residue, M′, when the exponentiated ciphertext is divided by the product of the two predetermined prime numbers associated with the intended receiver. The residue M′ corresponds to the original encoded message M.

40 Claims, 7 Drawing Figures

인증서 개념의 탄생 ('78)


Towards a Practical Public-key Cryptosystem

by

Loren M Kohnfelder

Submitted in Partial Fulfillment

of the Requirements for the

Degree of Bachelor of Science

at the

Massachusetts Institute of Technology

May, 1978

Signature of Author ______________________
Department of Electrical Engineering, May 10, 1978

Certified by ______________________
Thesis Supervisor

Accepted by ______________________
Chairman, Departmental Committee on Theses

ARCHIVES

MAY 25 1978

- Loren Kohnfelder – **Invention of Digital Certificates**
  - Loren Kohnfelder's B.S. thesis (MIT 1978, supervised by Len Adleman), proposed notion of digital certificate — a digitally signed message attesting to another party's public key.

[Note] MS's STRIDE Threat Model

The threats to our products

April 1, 1999 — By Loren Kohnfelder and Praerit Garg

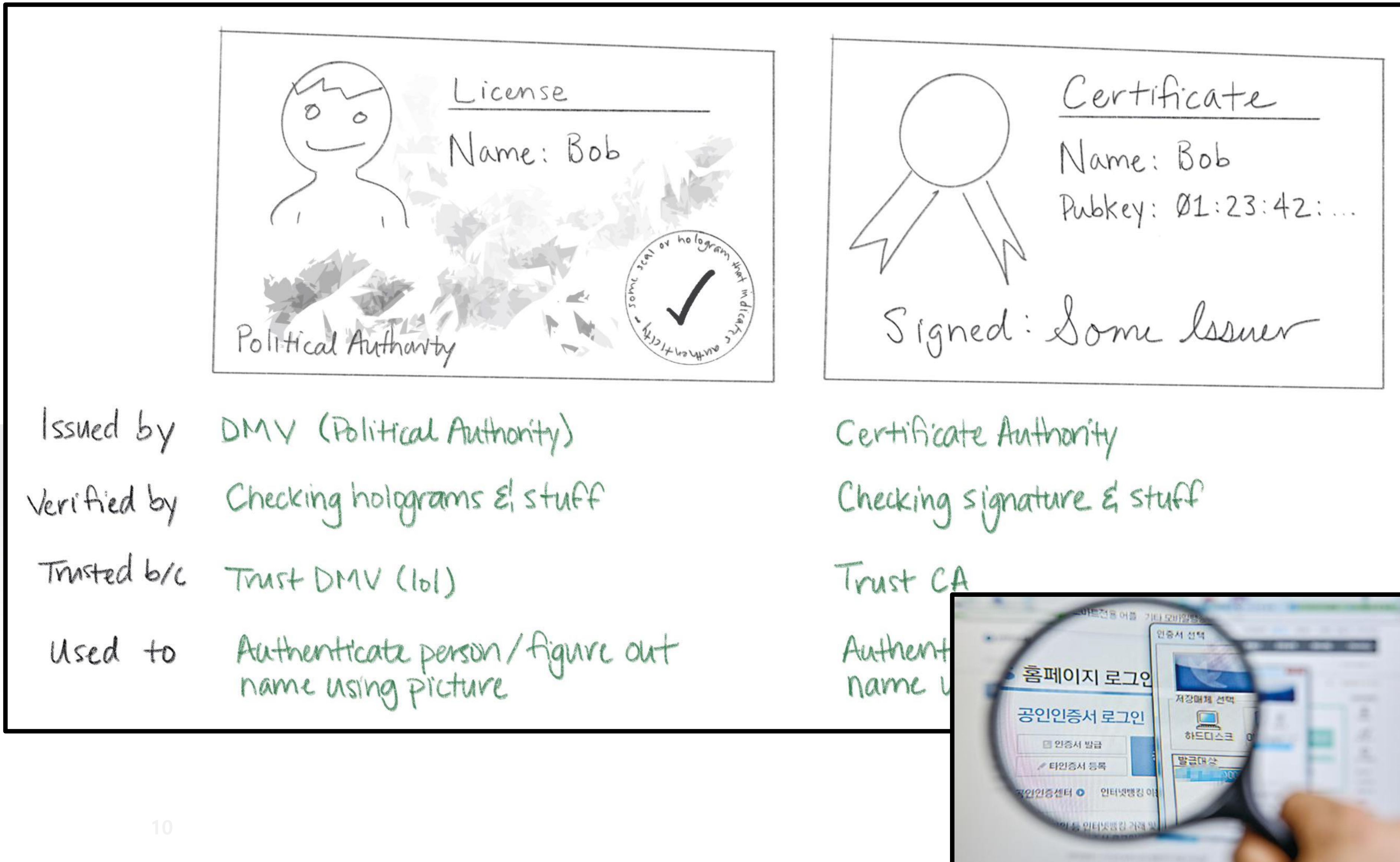
The growing use of computer systems to store data critical to businesses, as well as users' personal data, makes them very attractive targets for security attacks. Successful attacks can lead to loss of privacy, disclosure of sensitive data, and disruption or denial of service—losses that can cost millions of dollars. The Microsoft Security Task Force has defined a security threat model that it recommends all Microsoft product teams adopt to secure our products for our customers.

The **S.T.R.I.D.E.** security threat model should be used by all MS products to identify various types of threats the product is susceptible to during the design phase. Identifying the threats is the first step in a proactive security analysis process. Threats are identified based on the design of the product. The next steps in the process are identifying the vulnerabilities in the implementation and then taking measures to close security gaps.

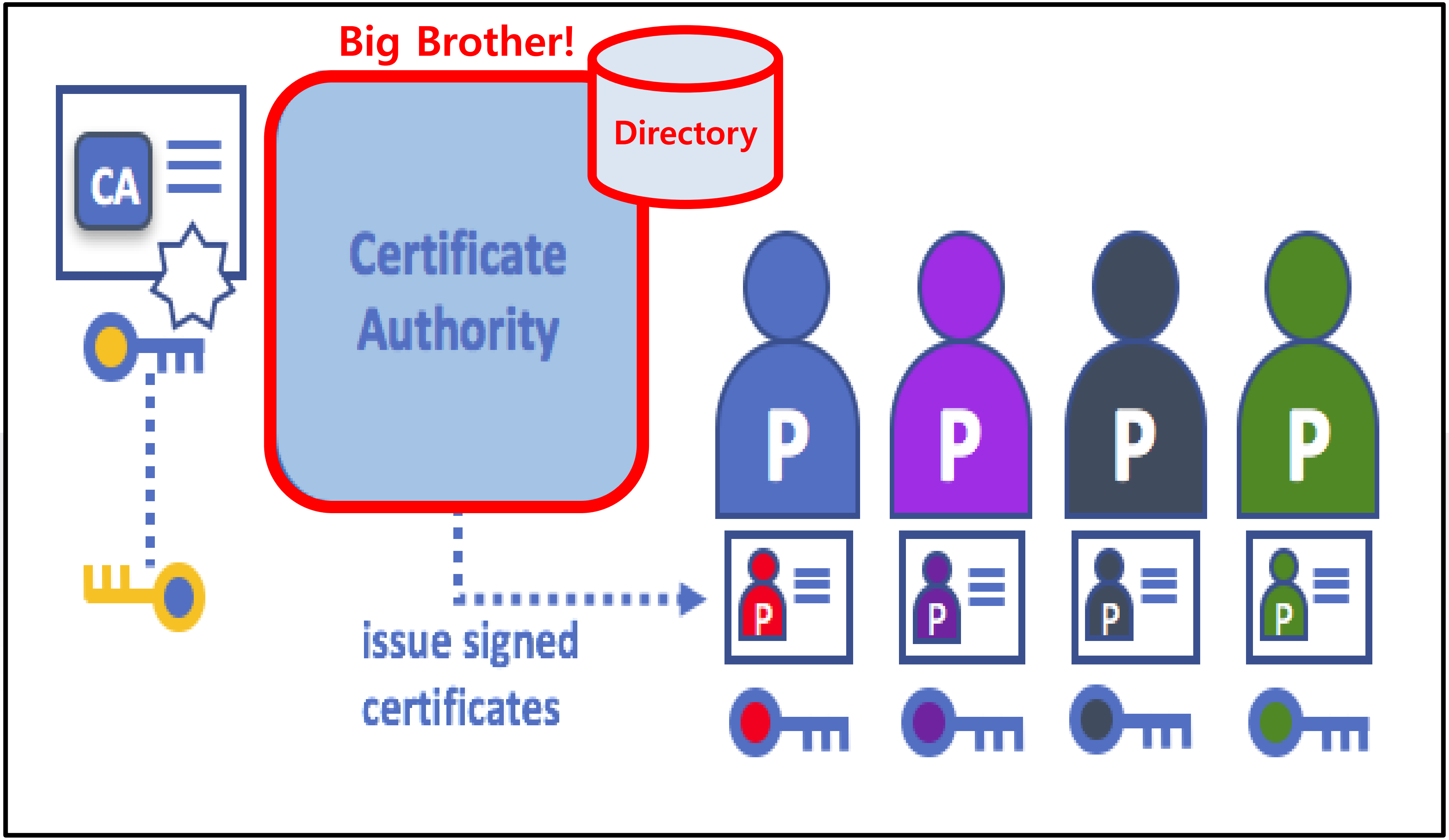
S.T.R.I.D.E. stands for:

- **Spoofing of user identity**
- **Tampering with data**
- **Repudiability**
- **Information disclosure (privacy breach)**
- **Denial of Service (D.o.S.)**
- **Elevation of privilege**

X.509 인증서

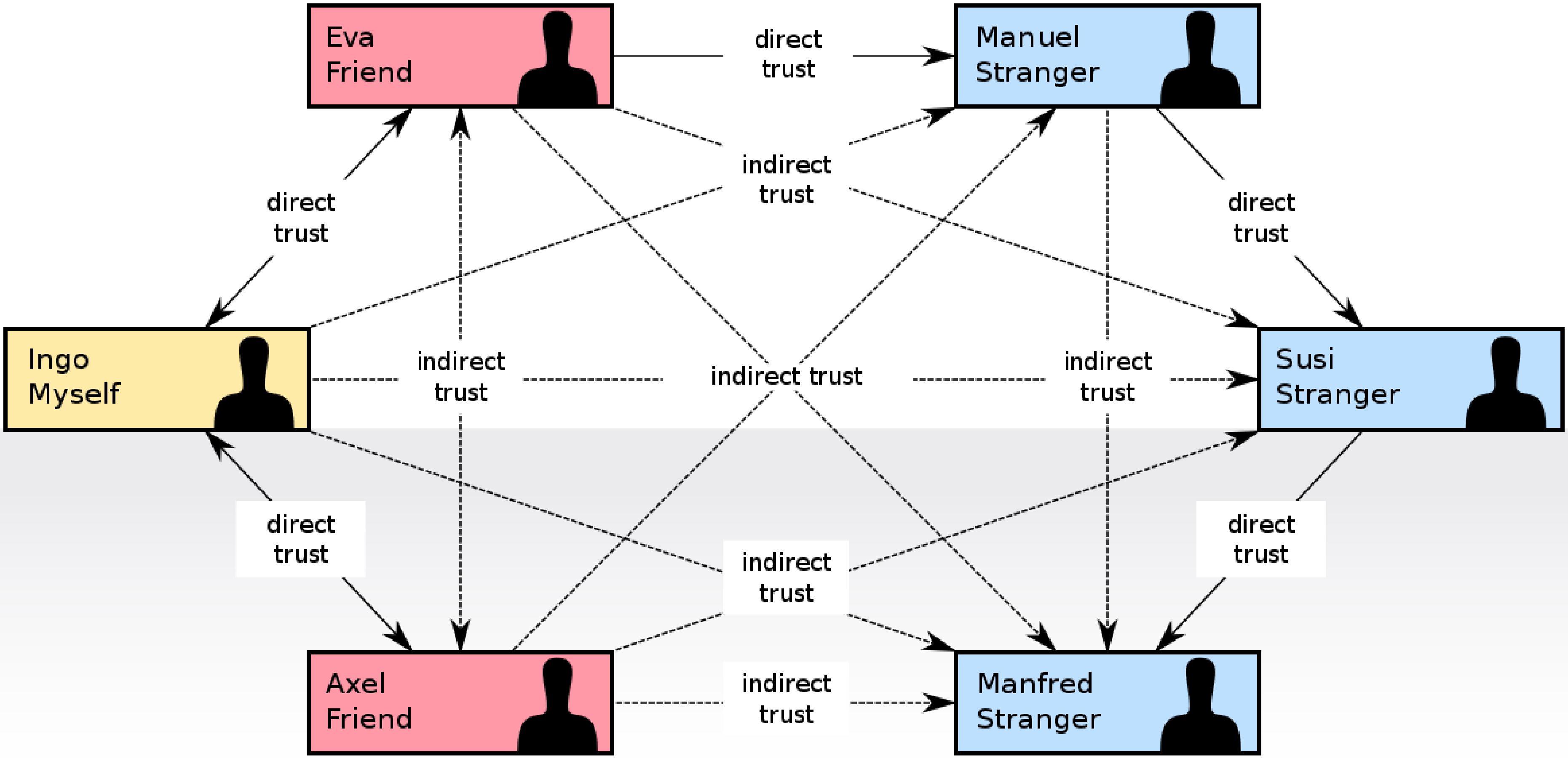

License
Name: Bob
Political Authority
some seal or hologram that indicates authenticity
Certificate
Name: Bob
Pubkey: 01:23:42:...
Signed: Some Issuer
Issued by
DMV (Political Authority)
Certificate Authority
Verified by
Checking holograms & stuff
Checking signature & stuff
Trusted b/c
Trust DMV (lol)
Trust CA
Used to
Authenticate person / figure out name using picture
홈페이지 로그인
공인인증서 로그인
인증서 발급
타인증서 등록
인증서 선택
저장매체 선택
하드디스크
발급대상

X.509 인증서



Big Brother!
CA
Directory
Certificate Authority
P
P
P
P
P
P
P
P
issue signed certificates

PGP : Web of Trust



Not Popular!

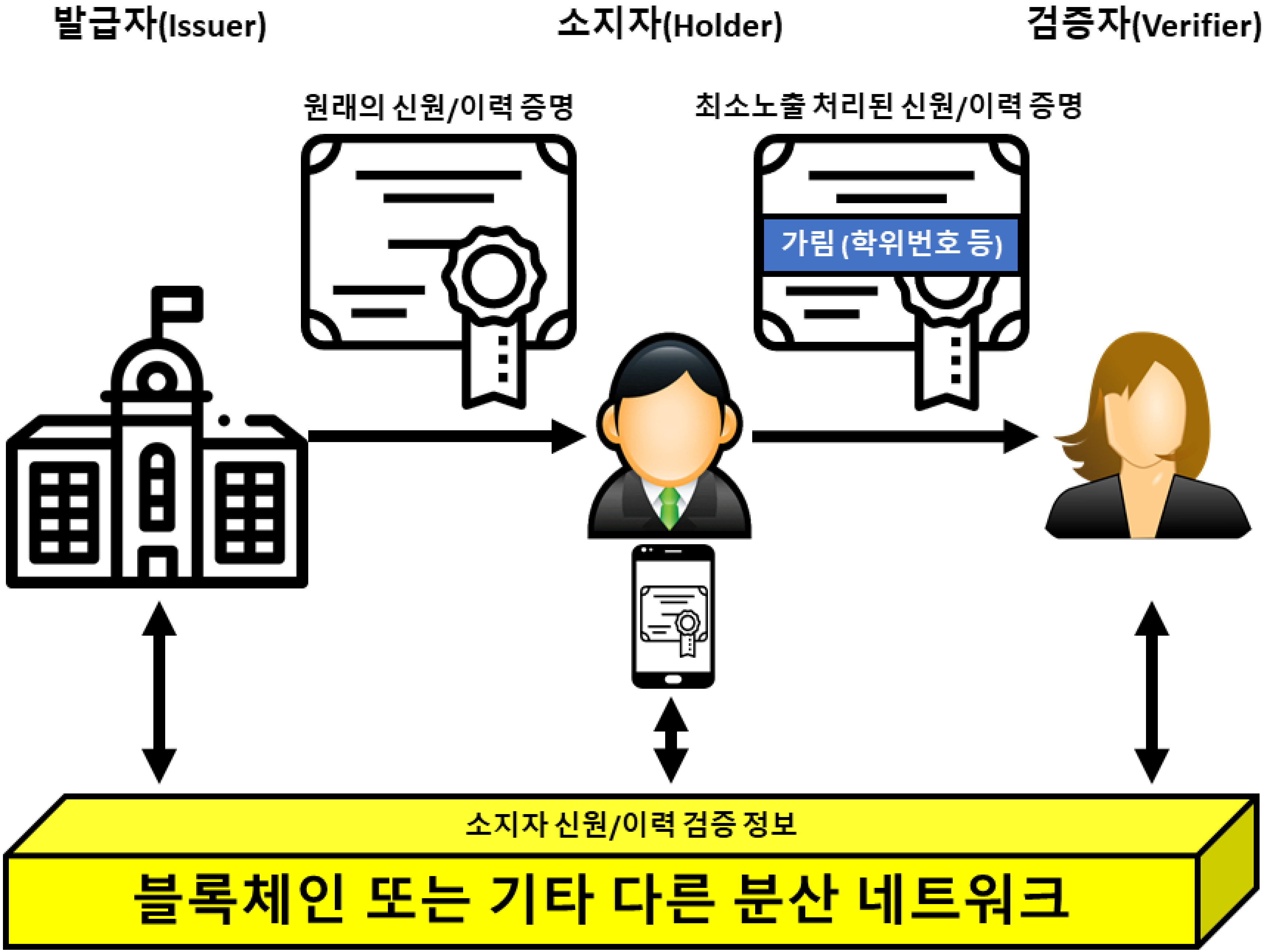
Bitcoin & Blockchain (2008)

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main

(In October 2008, posted to the Cypherpunks mailing list)



DID(Decentralized Identifiers)의 구조

① DID는 블록체인으로만 만들 수 있다?

Life With Alacrity

A blog on social software, collaboration, trust, security, privacy, and internet tools by Christopher Allen.

The Path to Self-Sovereign Identity

April 25 2016 – 4200 Words
by Christopher Allen

Today I head out to a month-long series of events associated with identity: I'm starting with the 22st (!) Internet Identity Workshop next week; then I'm speaking at the blockchain conference Consensus about

v

identity.

DID가 가져야 할 11개의 요구사항을 제시한바 있으며, 이는 현재 좋은 DID 서비스를 판별하는 주요 기준으로 활용되고 있음.

DID가 가져야 할 조건

- **Existence :** Users must have an independent existence.
- **Control :** Users must fully control their identities.
- **Access :** Users must have access to their own data.
- **Transparency :** The algorithms should be free, open-source, well-known, and as independent as possible of any particular architecture.
- **Persistence :** Identities must be long-lived.
- **Portability :** Information and services about identity must be transportable. It should not be held solely by a third party.
- **Interoperability :** Identities should be as globally usable as possible.
- **Consent :** Users must agree to the use of their identity. Users are in control of the sharing of their data.
- **Minimalization :** Disclosure of claims must be minimized.
- **Protection :** The rights of users must be protected.
- **Provable :** Identities and claims must have legal value.

DID와 관련한 가장 큰 오해 중 하나는 "DID는 블록체인으로만 구현할 수 있다"는 것임.

퍼블릭 블록체인을 이용할 경우, 블록체인이 갖는 고유의 특징으로 인해 DID가 가져야 할 11개의 특성 중 'Transparency'와 'Persistence', 'Interoperability' 성질을 달성하기가 쉬워질 뿐임.

(출처: DID에 대한 오해와 진실
https://amhoin.blog.me/221866951895)

Microsoft | Microsoft Tech Community   Community Hubs   Events   Blogs   Microsoft Learn   Lounge   Search the community   Sign In

Alex Simons (AZURE) Microsoft   05-13-2019 06:00 AM

Toward scalable decentralized identifier systems

"Today, we're announcing an early preview of a Sidetree-based DID network, called ION (Identity Overlay Network) which runs atop the Bitcoin blockchain."

That is until now. **Today, we're announcing an early preview of a Sidetree-based DID network, called ION *(Identity Overlay Network)* which runs atop the Bitcoin blockchain** based on an emerging set of open standards that we've developed working with many of our partners in the Decentralized Identity Foundation. This approach greatly improves the throughput of DID systems to achieve tens-of-thousands of operations per second.

I've asked Daniel Buchner, a program manager on my team who works on standards and open source solutions, to present our latest contributions in this area. His post introduces another major component we've been developing—in collaboration with other members from Decentralized Identity Foundation (Decentralized Identity Foundation (DIF)—to create a scalable foundational layer for decentralized identity systems.

As always, we'd love to hear your thoughts and feedback.

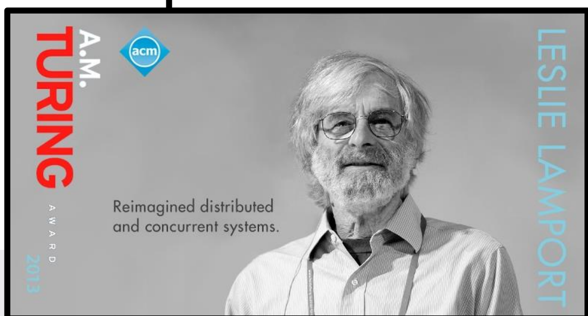
Best regards,

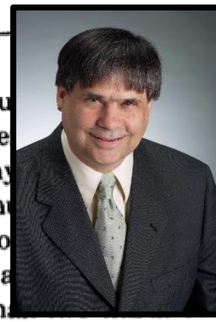
② DID는 해킹이 불가능하다

블록체인이란?

The Byzantine Generals Problem

LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE
SRI International





ms mu … ctioning components that give conflicting information
syste … n can be expressed abstractly in terms of a group of
army … ir troops around an enemy city. Communicating only
als m … common battle plan. However, one or more of them
try to … rs. The problem is to find an algorithm to ensure that
each … hown that, using only oral messages, this problem is
… ore th … he generals are loyal; so a single traitor can confound two loyal generals. With unforgeable written messages, the problem is solvable for any number of generals and possible traitors. Applications of the solutions to reliable computer systems are then discussed.

Categories and Subject Descriptors: C.2.4. [**Computer-Communication Networks**]: Distributed Systems—*network operating systems*; D.4.4 [**Operating Systems**]: Communications Management—*network communication*; D.4.5 [**Operating Systems**]: Reliability—*fault tolerance*

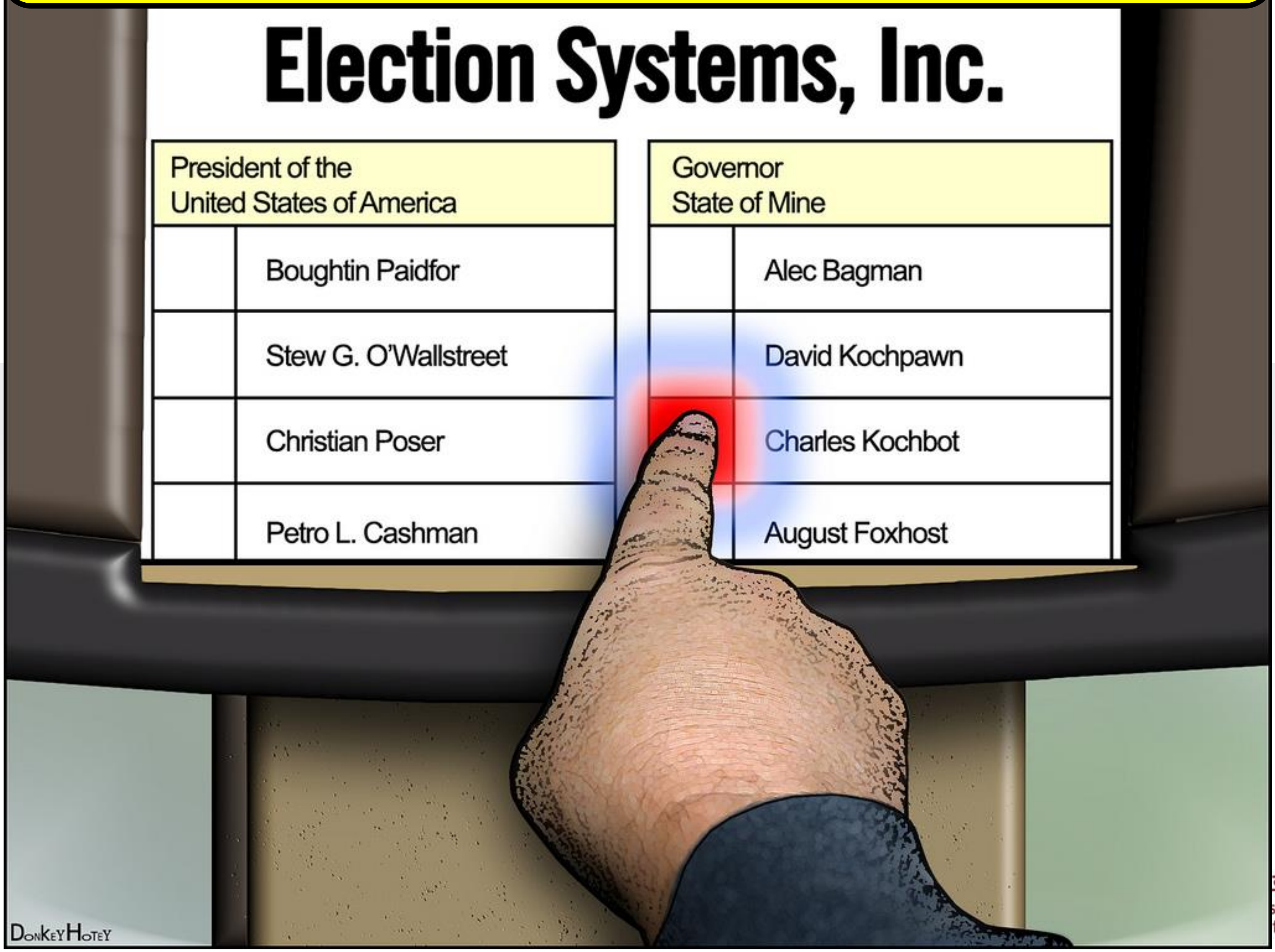
General Terms: Algorithms, Reliability

Additional Key Words and Phrases: Interactive consistency

(ACM Transactions on Programming Languages and Systems (TOPLAS), July 1982)

블록체인이란?

분산된 공개장부 + 투표 ⇒ Blockchain



블록체인은 해킹이 불가능한 기술이 아니며, 단지 ▲탈중앙성, ▲투명성, ▲불변성, ▲가용성의 기술적 특성만을 제공함.

그렇기에 블록체인 기반 DID의 경우, 신분증의 위조 방지에는 강점을 보이는 반면, **신분증 상에 기록된 개인정보의 노출에는 취약**함.

(출처: DID에 대한 오해와 진실
https://amhoin.blog.me/221866951895)

이러한 문제를 해결하고 더불어 'Minimalization(필요 최소한의 개인 정보만을 노출)' 조건을 충족시키기 위해, DID에서는 블록체인 이외에도 '영지식 증명(Zero-Knowledge Proofs) 기술'이 필수적임.

(출처: DID에 대한 오해와 진실
https://amhoin.blog.me/221866951895)

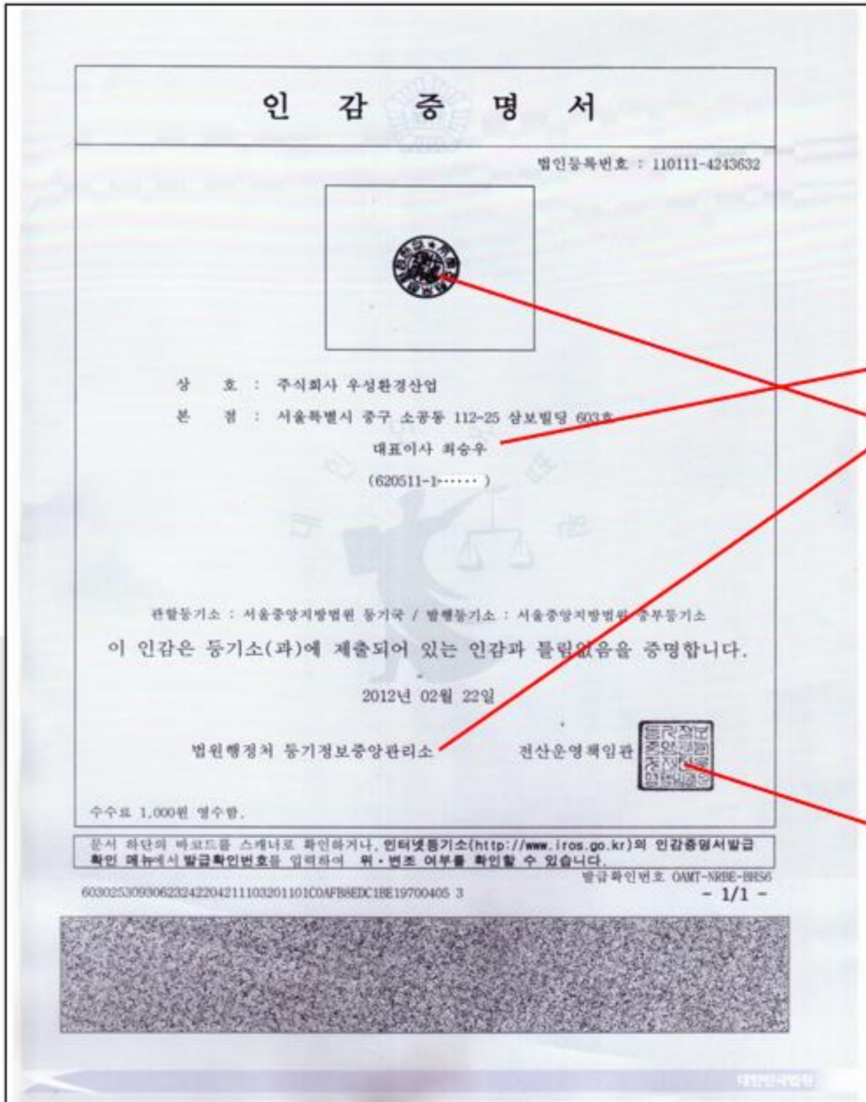
③ DID는 공인인증서를 대체할 수 있다?

공인인증서의 탄생 및 정권별 변천사

공인인증서란?

- 1999년 7월 **전자서명법**을 제정. 같은 해 9월 최초의 국내 표준 암호화 기술 '**SEED**' 발표.
  - '공인인증기관이 발급한 인증서에 기초한 전자서명'에 대해 법령이 정한 서명 또는 기명날인과 동등한 효력을 갖도록 했으며, 이때 공인인증기관의 지정은 정보통신부장관이 하도록 함.
- 2002년 4월에 법 개정.
  - 공인인증기관이 발급한 인증서 → **공인인증서**
  - 공인인증기관이 발급한 인증서에 기초한 전자서명 → **공인전자서명**

공인인증서란?


인 감 증 명 서

법인등록번호 : 110111-4243632

상 호 : 주식회사 우성환경산업

본 점 : 서울특별시 중구 소공동 112-25 삼보빌딩 603호

대표이사 최승우

(620511-1······)

관할등기소 : 서울중앙지방법원 등기국 / 발행등기소 : 서울중앙지방법원 중부등기소

이 인감은 등기소(과)에 제출되어 있는 인감과 틀림없음을 증명합니다.

2012년 02월 22일

법원행정처 등기정보중앙관리소 전산운영책임관

수수료 1,000원 영수함.

- 1/1 -

표 10-1 인증서의 규격 X.509 개요(그림 10-7의 밥의 인증서와 대응)

서명 전 인증서	
규격의 버전	3
인증서의 일련 번호	17:ab:4a:84:7d:6c:15:8e:79:4c:2e:e8:e8:26:7d:23:
디지털 서명의 알고리즘	md5WithRSAEncryption
인증서의 발행자	CrossCert Class 1 Consumer Individual Subscriber CA
유효 기한의 개시	Dec 24 00:00:00 2006 UTC
유효 기한의 종료	Feb 22 23:59:59 2007 UTC
공개 키의 소유자	GilDong Hong, /Email=gildong@novel.ac.kr
공개 키의 알고리즘	rsaEncryption
공개 키 본체	RSA Public Key: (1024 bit) Modulus (1024 bit): e3:08:47:05:ea:69:6c:ef:d9:8c:59:a0:79:fc:4a:84:a5:44:91:3b: 92:4c:1c:09:4e:e6:c6:fb:88:67:42:3e:bb:fe:75:75:b9:38:97:35: dc:6b:20:ca:07:2d:71:fa:fa:d5:18:51:f4:f7:b5:a0:87:17:1e:08: 3a:cb:be:23:f8:16:3d:a9:33:19:53:38:45:b7:e4:8a:31:65:5b:26: ac:d0:6a:46:c3:50:2d:b4:b2:bc:e0:16:fc:23:1d:39:8b:bd:93:0e: c1:ac:40:10:3f:e2:e8:4e:6e:20:88:6c:ab:24:b9:c5:5b:b1:fb:3f: 9a:10:46:0f:a1:57:9b:23: Exponent: 00:01:00:01:
확장 항목(생략)	
디지털 서명 알고리즘	md5WithRSAEncryption
디지털 서명 본체	68:90:36:be:d8:16:c5:74:fc:52:c7:5e:b0:43:6e:03:25:9a: e6:5e:6c:cb:dc:c1:11:c0:2a:70:de:ba:12:28:80:fa:9b:fa: 20:7f:e7:47:f6:11:21:a1:e6:d9:2a:3e:c4:8b:83:ce:d9:e4: 77:39:c1:61:0f:e5:4f:27:22:c1:ca:f5:29:73:8d:f0:58:48: 0e:75:28:0f:f6:9e:10:76:ca:8d:8d:09:04:84:fd:a6:38:5e: a9:f7:56:2d:fb:a8:23:dc:a4:45:58:bc:54:1b:17:67:c6:da: 8a:6b:ae:0e:71:db:7e:20:45:58:0c:67:97:de:00:8c:fb:51: e0:04:

공인전자서명이란? – NPKI vs. GPKI

막도장	인감도장	관인
		
사설인증	NPKI	GPKI

[Note] SEED란?

- 국내 보안산업의 '**씨앗**'이 되라는 뜻.
- 민간에서 암호가 **자유롭고** 널리 쓰이게 하자는 뜻.
- SEED가 오히려 지금은 민간분야에서 무조건 써야만 하는 mandatory 알고리즘으로 인식되고 있는 것은 잘못.

공인인증서를 대체하려면...

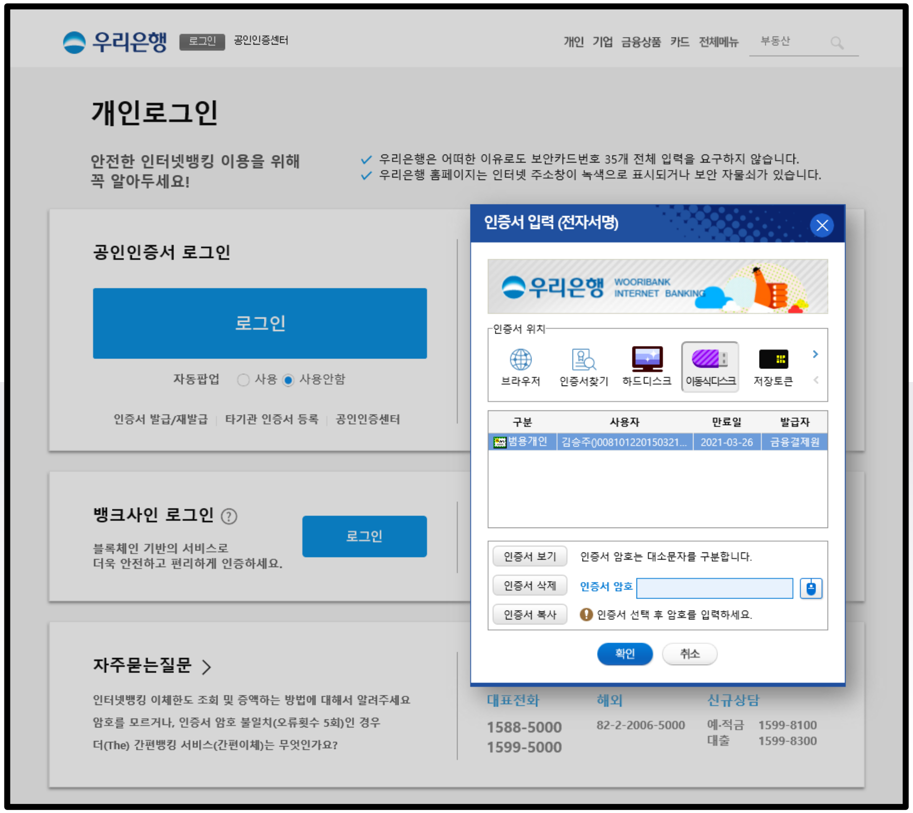
- 공인인증서는 **본인 확인** 기능 외에 **전자문서에 대한 결제** 기능까지도 동시에 제공할 수 있음.

  - 일반적으로 공인인증서의 본인 확인 기능을 대신할 수 있는 기술은 쉽게 찾을 수 있으나,

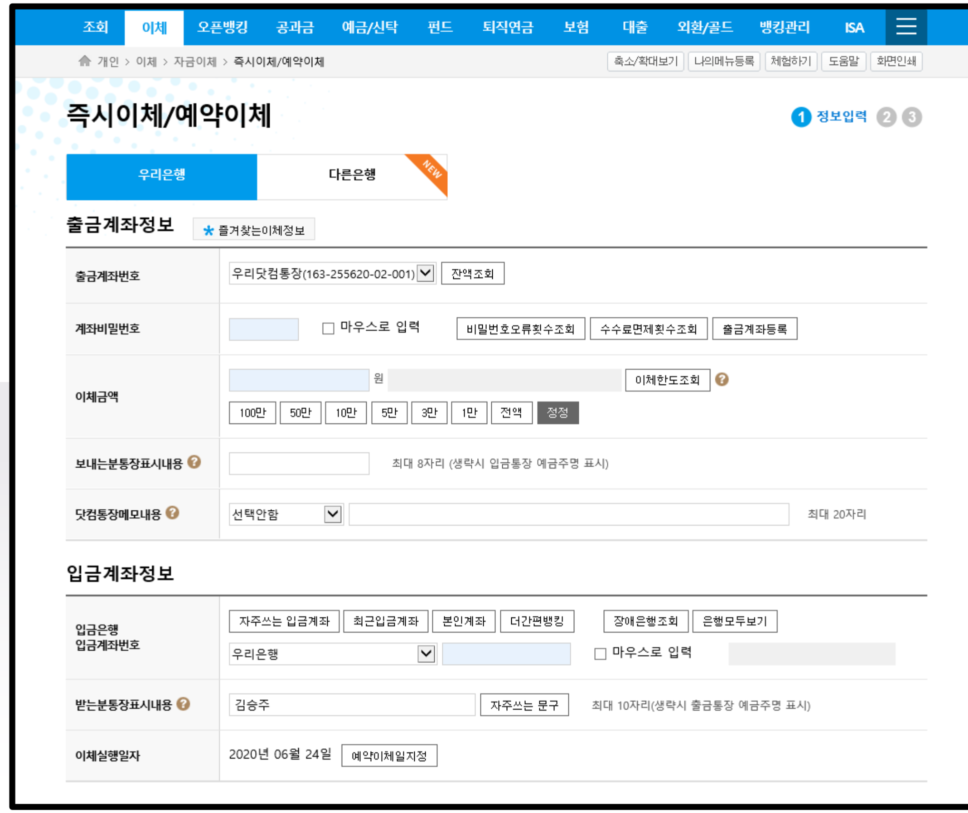
  - 공인인증서의 결제 기능 즉, 문서의 위·변조 및 거래사실의 부인 방지 기능까지도 대체하는 기술을 만들기란 쉽지 않음.

공인인증서를 대체하려면...

본인 신원 확인 (Easy)



문서의 위·변조 및 거래사실의 부인 방지



Keyless Signature Infrastructure and PKI: Hash-Tree Signatures in Pre- and Post-Quantum World

Ahto Buldas[2], Risto Laanoja[1,2], and Ahto Truu[1,2]

[1] Guardtime AS, Tammsaare tee 60, 11316 Tallinn, Estonia.
[2] Tallinn University of Technology, Ehitajate tee 5, 12618 Tallinn, Estonia.

Abstract. Multi-tenancy in the cloud environment brings new challenges to data security including but not limited to trust, data and system integrity and the overhead of cryptographic key management. These challenges can be efficiently addressed using novel data signing schemes.
We compare personal digital signature solutions provided by Public Key Infrastructure (PKI) and Keyless Signature Infrastructure (KSI) and describe how these technologies can support each other. We discuss some ways of integrating a personal KSI service with external Identity Providers. As KSI can "indemnify" PKI against the cryptographic threat of practical quantum computers, we delve into the post-quantum security of cryptographic hash functions and hash-and-publish signature schemes.

1 Introduction

Public Key Infrastructure (PKI) and Keyless Signature Infrastructure (KSI) are technologies intended to make electronic data more reliable by providing mechanisms for identifying the origin of data and to create irrefutable proofs that data was not modified since a certain time. While PKI relies on the continuous secrecy of private keys, which is necessary for the identification of the origin, KSI only relies on cryptographic properties of hash functions and the availability of widely published verification codes.

Keys are the weakest links in any secure system because they can be compromised owing to various factors–technical, human factors or both. In the creation process of personal electronic signatures, some types of pre-shared secrets (keys, passwords, etc.) seem unavoidable because secrets are necessary for authenticating the signer. This means that the validity of signatures depend on assumptions that some private keys are secure.

For example, the keys of Public Key Infrastructure (PKI) service providers like Online Certificate Status Protocol (OCSP) responders are used to sign the validity statements of public-key certificates.

Instant revocation has been a serious problem for traditional PKI signatures. On the one hand, revocation is necessary to protect the signer if there is a suspicion of leakage of the signature key. On the other hand, the possibility of revocation makes the signature verification procedure much more complex, because it must be proven that the key was not revoked at the time of signature creation. This means that many additional confirmations (such as OCSP responses, cryptographic time-stamps, etc.) must be added to the signature together with public-key certificates. Note that if instant revocation is possible, a signature key might be revoked right after signing, which means that electronic signature solutions must be very precise in determining the chronological order of the signing and revocation events. For some types of assets, such a determination must be possible decades after the assets have been signed.

KSI provides an alternative signature solution, where signing is *server-based*, i.e. signatures are created in assistance of *signature servers* that use the so-called hash-and-publish mechanism. The server creates

KSI Seal for Post-Quantum Indemnification Data containers described in preceding sections stay secure even if quantum computers emerge and all current PKI algorithms become insecure. This means that if we encapsulate all PKI signatures into KSI containers, the devastating effect of the quantum revolution is reduced dramatically because it is possible to show that signatures were created before the quantum computing was available and that data and PKI signatures were not tampered with before the KSI sealing.

Of course, after the quantum revolution, current modular arithmetic based signature schemes must be replaced with quantum-immune signature schemes, such as hash-based signatures.

This "indemnification" also provides long-term protection against other algorithm-related risks, like the development of new crypto-analytic attacks and inadequate security parameters (key length).

KSI as a Scalable Batch Signature Scheme KSI can be used to dramatically increase the power of PKI signature mechanisms. Even with the help of special-purpose hardware, the number of messages a service provider (say, an OCSP responder) can sign in a time unit is limited. To increase the volume, many devices that have a copy of the same private key are needed. KSI can help by offering a Merkle-tree based batch signature mechanism, wherein many messages are signed at a time so that the messages are first considered as the leaves of a hash tree and then the root hash computed and signed in a conventional way (e.g. RSA). Every message is then provided with a copy of the RSA signature and the corresponding hash chain. This way, the power of PKI signature devices can be increased tremendously without additional Hardware Security Modules (HSMs).

4.2 How PKI Supports KSI

Client Identification in KSI with PKI As described in Sec. 2.3, the identities of child servers are added to the hash tree by parent servers after a successful authentication. The same mechanism can be used at the first level of KSI wherein end-clients are authenticated by KSI gateways. There are several session and message-based mechanisms for authenticating clients, one of them requiring valid PKI signature on input data to KSI signing service.

If signing requests are PKI-signed, then KSI can be used for: (1) maintaining the key validity information and (2) creation of sustainable evidence containers that are free of major shortcomings of the PKI evidence containers.

If KSI service gateways that authenticate end-clients have access to fresh certificate validity data and perform functions similar to OCSP responders, the *instant revocation problem* is solved in a trivial way—if we assume that gateways receive revocation requests from clients and in case a client has announced the revocation of the signature key, the gateway no longer creates signatures for this client. Hence, a KSI signature itself is a proof of the validity of key, because otherwise, it would not have been created at all.

PKI as a Temporary Publication Mechanism in KSI The hash-and-publish mechanism used in the keyless signature system assumes periodic publishing of the global root hash values (the so-called *hash calendar*). As publishing is costly and cannot be done every second, there have to be some integrity check mechanisms in place for the time period starting from signature creation, ending with the next publication. A PKI signature is a suitable mechanism for such an integrity check. If the root hash values are signed with a service provider's private key and the public key has been reliably delivered to clients, KSI signatures become verifiable right after they have been created.

After the publication has been completed, PKI signatures can be superseded by hash chains from root

Blockchain = Decentralized Timestamping

≠ Digital Signature

마치며

- 데이터의 안전한 활용이 강조되는 4차 산업 혁명 시대에 DID에 대한 정부나 기업의 관심은 환영할 만한 일임.
- 그러나 그렇다고 해서 이를 **블록체인과 같은 특정 기반 기술과 과도하게 연결**짓거나,
- 신속한 사업 추진을 이유로 **정부나 기존 본인 확인기관들이 필요 이상으로 관여**하는 것은 곤란하며, 이는 오히려 바람직한 생태계 조성을 방해할 수도 있음.

NetSec-KR

DID에 대한 오해와 진실

고려대학교 정보보호대학원 교수

국방 RMF 연구센터(AR^{2}C) 센터장

고신뢰 보안운영체제 연구센터(CHAOS) 센터장

김 승 주 (Seungjoo Kim)

(FB) www.fb.com/skim71 (Twitter) @skim71

고려대학교 정보보호학부 · 정보보호대학원

Korea University Division of Information Security

Graduate School of Information Security