인증서를 이용한 개인식별번호 확인 및 키분배 통합 프로토콜

김 성 덕[†] · 정 재 동[††] · 원 동 호[†††]

요 약

기존의 인증서를 이용한 사용자 인증(Authentication) 또는 개인식별(Identification)은 인증서의 공개키에 대응하는 비밀키의 소유자가 인증서의 소유자 필드에 설정된 DN의 사용자임을 확인하는 과정에 한정되며, 인증서의 실 소유자가 실세계의 누군인가를 파악할 수 없다는 문제점이 있었다. 이를 보완하기 위해 인증서 소유자의 주민등록번호와 같은 식별번호를 인증서 확장필드에 안전하게 포함시키는 방법이 기술규격으로 만들어져 국내 공인인증체계에 적용되고 있다. 본 논문에서는 ECC 암호알고리즘을 이용하여 사이트 로그인과정에서 개인식별, 키분배, 그리고 식별번호를 이용한 소유자 확인이 가능한 통합 프로토콜을 제안한다.

키워드 : 개인식별, 키분배, 통합프로토콜

The Integrated Identification Number Checking and Key Management Protocol with Certificates

Kim Sung Duk[†] · Jung Jae Dong[††] · Won Dong Ho[†††]

ABSTRACT

The existing certificate based authentication or identification just verifies whether the owner of private key corresponding to public key of certificate is the DN user set in the user field in the certificate or not, then we cannot find out who is the actual private key owner in a real world. To make up for this weak points, the method to insert the identification number like the resident registration number into the certificate extension field is applied as a technical standard to current domestic PKI system. In this paper, we propose the ECC based integrated identification, identification number checking and key management protocol providing user validation during the login.

Key Words : Identification, Key Management, Integrated Protocol

1. 서 론

X.509 표준에서는 공개키 인증서(Public Key Certificate)를 "DN(Distinguished Name)으로 표시되는 소유자와 소유자의 공개키 사이의 연관성을 증명하기 위하여, 제3의 신뢰기관이 관련된 내용에 대해 전자서명을 하여 공개한 정보"라고 정의하고 있다. 또한, 공개키기반구조(PKI : Public Key Infrastructure)는 "최상위 인증기관 및 하위 인증기관, 그리고, 인증서 소유자간의 신뢰관계를 정의하고, 상위 인증기관의 전자서명을 이용하여 하위 인증기관이나 일반 사용자의 인증서에 포함된 공개키와 소유자간의 연관성을 확인하는 방법"으로 정의하고 있다[1, 2].

지금까지 개발된 각종 표준과 기술을 통해 인증서의 소유자(Subject) 필드에 DN으로 표시되는 인증서 소유자와 공개키의 연관성을 증명하는 것은 별다른 문제가 없지만, 공개키 인증서는 인증서 소유자의 DN과 공개키 사이의 연관성만을 증명하기 때문에, 공개키 인증서만으로 인증서 소유자가 현실 세계의 누구인지를 파악할 수는 없다.

공개키 인증서 소유자에 대한 정보가 Subject필드와 확장필드인 사용자대체명(Subject Alternative Name)에 저장되기는 하지만, DN의 CN(Common Name)과 OU(Organization Name) 등의 형식으로 표시되는 정보는 공개키 인증서 소유자와 인증기관의 환경에 의해 수시로 변경될 수 있는 정보이고, 동일환경에서 동일한 이름을 갖는 사람이 복수일 수 있다는 점에서 인증기관의 개입이 없이 공개키 인증서를 이용하여 소유자를 정확하게 구분하기는 힘들다는 단점이

† 준 회 원 : 성균관대학교 정보통신공학부 정보보호연구실 박사과정
†† 정 회 원 : 한국증권전산(주) 시스템사업본부 본부장
††† 종신회원 : 성균관대학교 정보통신공학부 교수
논문접수 : 2005년 2월 18일, 심사완료 : 2005년 4월 4일

있다. 이를 보완하기 위해서는 인증서와 인증서 소유자를 명확하게 연결시킬 수 있는 별도의 정보체계가 필요하다.

인증서 소유자의 식별 문제를 해결하기 위해서는 정부와 같이 공신력 있는 기관에서 개인과 법인에 고유한 정보를 부여할 수 있는 식별번호 체계를 구축하고, 식별번호를 인증서에 저장하는 방법이 가장 간단하면서도 안전하다. 이런 고유한 식별정보가 있다면, 인증서 수신자는 인증서에 포함된 Subject 필드와 식별번호를 이용하여 인증서 소유자를 정확하게 구분할 수 있다. 최근에 IETF에서는 인증서의 이런 문제점을 해결하기 위해 각 인증서에 인증서 소유자에 대한 영구적인 식별번호를 저장하는 방법에 대해 논의하고 있다[4].

한국에는 이러한 식별번호로 주민등록번호와 사업자등록번호가 오래 전부터 구축되어 사용되고 있다. 대부분의 서비스 회사는 이런 식별번호를 이용하여 고객을 구분하고 고객에 맞는 서비스를 제공하고 있다. 이는 통신 및 컴퓨터 기술이 도입되기 이전부터 사용하던 방법이므로, 지금까지 구축된 대부분의 데이터베이스에서 주민등록번호 또는 사업자등록번호를 고객을 관리하는 키(Primary Key)로 사용하고 있다고 해도 과언이 아니다.

하지만, 식별번호는 개인정보로 분류되고, 관례적으로 비밀번호(Password)와 유사한 기능을 수행하여 왔기 때문에, 소유자의 허가가 없이 식별번호를 제 3자에게 알려주는 것은 불법으로 규정되어 있다. 주민등록번호의 경우, 이를 기준으로 많은 중요한 데이터베이스가 구축되어 있기 때문에 주민등록번호가 타인에게 알려지면, 많은 개인정보가 유출되는 시발점이 될 수 있으므로, 공개키 인증서와 같이 공개되는 정보에 주민등록번호를 그대로 저장하여 공개할 수는 없다.

이런 문제를 해결하기 위해, 한국정보보호진흥원은 인증서를 이용하여 식별번호를 확인할 수 있는 본인확인 기술규격을 정의하였다. 이 규격은 사용자의 식별번호와 안전한 길이의 난수를 해쉬함수에 입력하여, 그 결과값을 인증서 확장필드에 저장한다. 인증서 소유자가 서버에 접속하여 자신의 식별번호와 저장해 둔 난수를 서버에 보내고, 서버는 두 값을 해쉬함수에 입력하여 인증서에 저장되어 있는 값과 해쉬함수의 결과값이 동일한 가를 확인하면, 인증서 소유자의 식별번호를 확인할 수 있다[5].

일반적으로 인증서가 사용되는 인터넷 서비스의 로그인 절차를 살펴보면, 로그인 과정에서 암호 알고리즘과 프로토콜을 통하여 개인식별(Identification)이 이루어진 후, 인증서에 안전하게 저장된 식별정보를 이용하여 인증서 소유자의 식별번호를 확인하게 되며, 중요한 정보의 상호교환을 위해 세션키를 교환하거나, SSL 등을 이용하여 안전한 통신채널을 형성하는 3단계의 과정을 거치게 된다. 따라서, 이런 3개의 과정을 통합한 프로토콜이 있다면 좀 더 효율적일 것이다[8-11].

본 논문 2장에서는 한국정보보호진흥원에서 발표한 인증서를 이용한 개인식별정보 확인 프로토콜을 살펴보고, 3장에서는 타원곡선에 기반한 공개키 암호시스템을 이용하여, 인증서를 통해 개인식별, 식별번호를 이용한 본인확인 및 클래스 3 수준의 세션키 공유과정을 통합한 프로토콜을 제안하며, 4장에서는 제안된 프로토콜의 효율성에 대해 설명한 후, 5장에서 결론을 맺는다.

본 논문에서 사용하는 기호 및 용어는 다음과 같다.

- ID : 개인을 식별할 수 있는 신뢰할 수 있는 정보(예 : 주민등록번호)
- G : 타원곡선의 베이스 포인트
- X_A : 160 비트 이상(공인인증체계 기준)의 난수로 구성된 비밀키
- Y_A : $Y_A = X_A G$로 계산된 공개키
- K_S : POP 값을 생성하기 위한 160비트 이상의 난수
- $Sign_{X_A}(Message)$: A의 비밀키 X_A로 Message에 대한 전자서명을 생성
- POP : 비밀키 소유 증명을 위한 전자서명값
- V : 식별번호 확인을 위한 본인확인정보
- EV : 수신자의 공개키로 암호화된 본인확인정보)
- K_{ID} : 식별번호 확인용 160비트 이상의 난수
- $ENC_{Key}(PlainText)$: 공개키암호화 방식 또는 비밀키 암호화방식의 알고리즘으로 Key를 이용하여 PlainText를 암호화
- $DEC_{Key}(CipherText)$: 공개키암호화 방식 또는 비밀키 암호화방식의 알고리즘으로 Key를 이용하여 Cipher Text를 복호화

2. 기존 개인식별정보를 이용한 본인확인 프로토콜

한국정보보호진흥원에서 공개한 개인식별정보를 이용한 본인확인 과정은 개인식별정보를 인증서에 안전하게 저장하는 단계와 인증서 소유자가 비밀정보를 이용하여 인증서 수신자에게 개인식별정보를 증명하는 단계로 구성된다.

2.1 식별번호를 안전하게 인증서에 저장하는 과정((그림 1) 참조)

(1) 인증서 신청자는 비밀키(X_A)와 공개키(Y_A)를 생성하고, 난수(K_S)를 이용하여 POP(Proof Of Possession) 정보를 생성한다[3].

(2) 인증서 신청자는 식별번호 보호에 사용할 난수(K_{ID})를 생성한 후, 인증기관의 공개키로 신청자의 식별번호와 난수(K_{ID})를 암호화하여 EID를 생성한다.

(3) 인증서 신청자는 인증기관에 접속하여, 인증기관의 공개키로 안전한 통신채널(예 : SSL)을 생성한 후, 인증기관에 공개키, POP 정보, EID를 전달한다.

(4) 인증서 신청자는 비밀키(X_A)와 식별번호용 난수(K_{ID})를 안전하게 암호화하여 저장한다.

(5) 인증기관은 신청자가 보내온 정보 중, 공개키(Y_A)를 이용하여 POP를 검증하고, 인증기관의 비밀키(X_{CA})

신청자(A)	Y_{CA}	인증기관(CA)
X_A, K_S, K_{ID} : 난수 (160비트 이상) Y_{CA} : 인증기관키분배용공개키 $POP = Sign_{X_A}(K_S)$ $EID = ENC_{Y_{CA}}(K_{ID}, ID)$ K_{ID}와 X_A는 같이 저장	Ks $\rightarrow Y_A \rightarrow$ POP EID	Ks, Y_A를 이용한 POP검증 K_{ID}, $ID = DEC_{X_{CA}}(EID)$ DB의 ID와 동일한가 확인 $V = h(K_{ID}, ID)$ V를 인증서에 저장

(그림 1) 식별번호 설정과정

인증서 소유자(A)	Y_A, Y_S	서비스 서버(S)
Y_S : 서비스기관키분배용공개키 $EV = ENC_{Y_S}(K_{ID}, ID)$	$\rightarrow EV \rightarrow$	K_{ID}, $ID = DEC_{X_S}(EV)$ $V' = h(K_{ID}, ID)$ V'와 인증서의 V를 비교

(그림 2) 식별번호 확인과정

를 이용하여 복호화한 후, 신청자의 식별번호(ID)와 난수(K_{ID})를 해쉬하여 본인확인정보(V)를 생성한다.

(6) 인증기관은 본인확인정보(V)와 공개키(Y_A)가 저장된 인증서를 생성하여 신청자에게 전달한다.

2.2 식별번호확인 과정((그림 2) 참조)

(1) 인증서 소유자는 서비스 서버에 접속한 후, 서버의 공개키(Y_S)를 이용하여, 식별번호(ID)와 식별번호용 난수(K_{ID})를 암호화한 후, 서비스 서버에 전달한다.

(2) 서비스 서버는 인증서 소유자가 보내온 암호화된 정보를 자신의 비밀키(X_S)로 복호화 한 후, 인증서 소유자의 식별번호(ID)와 식별번호용 난수(K_{ID})를 추출한다.

(3) 서비스 서버는 인증서 소유자의 식별번호와 식별번호용 난수(K_{ID})를 해쉬한 결과가 인증서의 본인확인정보(V)와 동일한가 확인하여, 인증서 소유자가 보내온 식별번호가 맞는 다는 것을 확인할 수 있다.

2.3 문제점

지금까지 살펴본 기술규격은 실제 서비스 적용에 있어 다음과 같은 단점을 가지고 있다.

2.3.1 Man in middle 공격

인증서 소유자의 본인확인을 수행한 서비스 기관은 다른 서버에 동일한 정보를 보내, 인증서 소유자와 동일하게 행동할 수 있으므로 상기의 프로토콜은 Man in middle 공격에 취약하다고 할 수 있다. 이를 방지하려면, 인증서 소유자의 비밀키와 일회용 난수가 사용되는 과정이 통합되어야 한다.

2.3.2 통신 및 계산과정의 부담

현재 한국정보보호진흥원의 기술규격은 로그인 과정과 식별번호를 확인하는 과정간의 연관성을 규정하고 있지 않기 때문에, 별도의 개인식별 과정을 통한 로그인 후에 기술규격의 방법을 이용하여 식별번호를 다시 확인해야 하므로, 중복된 통신과정과 암호학적 계산과정이 추가로 필요하다.

2.3.3 별도의 키분배과정 및 인증수준

기술규격에는 식별번호(ID)와 식별번호용 난수(K_{ID})를 안전하게 서비스 서버에 전달해야 한다고 규정되어 있지만, 정확한 방법에 대해서는 정의하고 있지 않다. 일반적으로 서비스 서버에 접속하면 안전하게 정보를 송수신해야 하는 경우가 발생하는데, 이를 위해서는 키분배 과정이 필요하므로, 암호화세션을 위한 키분배가 사전에 형성되어, 본인확인과 중요한 정보 송수신에 모두 사용되는 것이 바람직하고, 클래스 3 수준의 상호인증이 이루어지는 것이 타당하다[7].

3. 통합 프로토콜의 제안

본 장에서는 ECC 기반의 공개키 암호시스템을 이용하여 식별번호를 통해 안전하게 본인을 확인하고, 비밀키를 이용하여 인증(Authentication)이 아닌 개인식별(Identification) 수준에서 인증서 소유자를 확인할 수 있으며, 서버와 클라이언트 상호간에 인증을 동시에 수행하는 클래스 3 수준의 키분배를 수행할 수 있는 프로토콜을 제안한다[6, 7]. 제안하는 프로토콜 또한 인증서에 개인식별정보를 저장하는 단계와 이를 이용하여 로그인 과정에서 인증서 소유자의 본인확인, 개인식별, 키분배를 수행하는 단계로 구분된다.

신청자(A)	Y_{CA}	인증기관(CA)
K_{ID} : *random* X_A : 비밀키, Y_A : 공개키 $Y_A = X_A * G$ $T = K_{ID} * X_A * Y_{CA}$ $POP = Sign_{X_A}(T)$ K_{ID}^{-1}는 X_A와 같이 저장	Y_A → POP→ T	T, Y_A를 이용한 POP검증 A의 ID를 DB에서 추출 $EV = T * ID^{-1} * X_{CA}^{-1}$ EV를 인증서에 저장

(그림 3) 식별번호 설정과정

인증서 소유자(A)	Y_S, Y_A	서버(S)
X_A, K_{ID}^{-1} 추출 $V_1 = h(X_A^{-1} * T_1 - Y_S)$ $T_2 = K_{ID}^{-1}(ID + V_1 * X_A^{-1})$ $T_3 = ENC_{V_1}(ID \| T_2)$	Y_A → 로그인→ 요청 ← T_1← → T_3→	r : *random* $T_1 = (X_S + r) * Y_A$ $V_1' = h(r * G)$ $ID \| T_2 = DEC_{V_1'}(T_3)$ 인증서의 EV 추출 $T_2 * EV = (ID^{-1} * V_1')G + Y_A$

(그림 4) 식별번호 확인과정

3.1 개인식별정보 반영

(1) 신청자는 비밀키(X_A)를 생성하고, 식별번호(ID)를 보호하기 위한 160비트 이상의 비밀정보(K_{ID})를 생성한다.

(2) 신청자는 인증기관의 인증서에서 인증기관 공개키(Y_{CA})를 추출한 후, 자신의 비밀키(X_A)와 식별번호용 난수(K_{ID})를 곱하여 임시정보(T)를 생성한 다음, 비밀키(X_A)로 임시정보에 전자서명하여 POP값을 생성하고, 공개키(Y_A), POP, 임시정보(T)를 인증기관에 전달한다.

(3) 신청자는 비밀키(X_A)와 식별번호용 난수(K_{ID})를 암호화하여 안전하게 저장한다.

(4) 인증기관은 인증서 신청자가 보내온 임시정보(T)에 대한 전자서명 POP를 인증서 신청자의 공개키(Y_A)로 검증한 다음, 신청자의 식별번호(ID)를 데이터베이스에서 추출하고, 신청자가 보내온 임시정보(T)값에 인증기관의 비밀키(X_{CA})의 역수를 곱한 후, 식별번호(ID)의 역수를 곱한 값 EV를 포함한 인증서를 생성하여 신청자에게 전달한다.

3.2 개인식별, 소유자 본인확인 및 세션키 교환

(1) 인증서 소유자가 서버에 로그인을 시도하면, 서비스 서버는 160비트 이상의 난수 r을 선택한 후, 인증서 소유자의 공개키(Y_A)에 서버의 비밀키(X_S)와 난수 r을 곱한 값 T_1을 인증서 소유자에게 보낸다.

(2) 인증서 소유자는 T_1을 받은 후, 비밀키(X_A)와 식별번호용 난수(K_{ID})를 복호화하여, T_1에 비밀키(X_A)를 곱한 후, 서버의 공개키(Y_S) 값을 빼서 생긴 값을 해쉬하여, V_1을 생성한다.

(3) 인증서 소유자는 비밀키(X_A)의 역수와 V_1값을 곱한 후, 식별번호(ID)를 더한 값에 비밀정보(K_{ID})의 역수를 곱하여 개인식별용 정보(T_2)를 생성한다.

(4) 인증서 소유자는 V_1 값을 이용하여 자신의 식별번호(ID)와 개인식별용 정보(T_2)를 암호화하여 T_3를 생성한다.

(5) 인증서 소유자는 T_3를 서버에 전달한다.

(6) 서버는 난수 r을 G에 곱한 후 이를 해쉬하여, V_1값을 계산한 후, T_3값을 복호화하여 신청자의 식별번호(ID)와 개인식별용 정보(T_2)를 복호화 한다.

(7) 서버는 신청자의 인증서에서 EV값을 추출한 후, 개인식별용 정보(T_2)와 곱한다.

(8) 서버는 (6)에서 복호화한 신청자의 식별번호(ID)의 역수와, (6)의 V_1값을 곱한 후, 그 값을 G값과 곱한다. 그리고 계산된 값과 신청자의 공개키를 더한다.

(9) (7)에서 계산된 포인트와 (8)에서 계산된 포인트의 값이 동일하다면, 신청자가 보내온 개인식별정보(ID)가 정확하고, 신청자 A에 대한 개인식별이 안전하게 이루어졌음을 확신할 수 있으며, 인증서 소유자와 서버 사이의 세션키 V가 공유되게 된다.

4. 장단점 분석

4.1 본인확인정보 생성과정

<표 1>에서 볼 수 있는 것과 같이 본 논문에서 제안하는 프로토콜의 가장 큰 특징은 별도의 암호화 세션을 구축하기 위한 절차가 프로토콜에 통합되어 있다는 점이다.

〈표 1〉 방식의 비교

구분	암호화세션	신청자 계산량	인증기관 계산량
기존방법	필요	암호화세션생성(1) 암호화(1)	암호화세션생성(1) 복호화(1), 해쉬(1)
제안방법	필요없음	Scalar 곱셈(1), 역수(1)	Scalar 곱셈(1), 역수(2)

한국정보보호진흥원의 기술규격에서는 인증서 신청자가 식별번호(ID)와 식별번호용 난수(K_{ID})를 인증기관에 안전하게 전송해야 하기 때문에 별도의 암호화 세션을 생성해야 하지만, 제안하는 방법은 프로토콜에 암호화 세션 생성절차가 통합되어 있기 때문에 암호화 세션을 구성하기 위한 서버와의 추가 통신 및 계산과정이 필요없다.

계산량 측면에서 암호화 세션을 생성하는 방법에 따라 차이가 있을 수 있지만, 역수의 계산이 사전계산으로 가능하며, 신청자와 인증기관 모두 Scalar 곱셈을 한번씩만 수행하면 된다. 또한, 임시정보 T의 무결성을 전자서명으로 생성된 POP정보를 이용하여 확인할 수 있다는 특징이 있다.

4.2 본인확인과정의 특징

4.2.1 Man in middle 공격의 방지

한국정보보호진흥원 기술규격의 방법은 난수(R)와 식별번호에 대한 해쉬함수 처리 결과을 이용하기 때문에 난수(R)와 식별번호를 아는 사람이 다른 사람에게 인증서 소유자인 것처럼 행동을 할 수 있는 Man in middle 공격에 약점이 있다. 이를 방지하려면 별도의 개인식별과정이 병행되어야 한다. 하지만, 제안하는 방법은 클라이언트 인증서 소유자의 비밀키(X_A)와 서버의 난수(T_1)가 계산과정에 사용되기 때문에 별도의 개인식별과정 없이 클라이언트와 서버가 상호 인증을 수행하는 클래스 3 수준의 인증이 가능하다

4.2.2 다기능의 통합

제안하는 프로토콜을 이용하여 사이트에 로그인 하는 경우, 서버가 클라이언트의 공개키를 이용할 수 있는 정보(T_1)를 보내고 클라이언트는 이것을 이용하여 암호화에 사용하는 키(V_1)를 생성하기 때문에 암호화 세션의 생성, 본인확인, 서로(서버, 클라이언트)간의 인증을 모두 수행할 수 있으므로 하나의 프로로콜 수행으로 세션의 생성/확인/관리에 필요한 대부분의 정보를 클라이언트와 서버가 공유할 수 있는 장점이 있다.

5. 결 론

본 논문에서는 공개키 인증서와 인증서 소유자의 관계를 증명하기 위해서 별도의 식별번호를 이용하는 방법에 기반하여, 로그인, 개인식별, 키분배를 동시에 해결할 수 있는 방법을 제안하였고, 제안한 방법의 효율성과 특징을 살펴보았다.

본 논문에서 제안한 방법은 웹 서비스 등 클라이언트-서버환경의 세션 생성/확인/관리 과정에서 필요한 사용자 확인, 암호화 세션 생성, Man in middle 공격의 방지를 한 번에 수행할 수 있다는 장점이 있어 현실적으로 사용이 가능할 것으로 판단된다.

또한, 타원곡선에 기반한 공개키 암호시스템을 기반으로 하기 때문에 일반 인터넷 환경과 개인용 컴퓨터는 물론, 계산능력이 부족한 단말기를 많이 사용하는 무선환경에서도 효율적으로 사용할 수 있을 것으로 판단된다.

참 고 문 헌

[1] X.509 4th Draft 8, The directory : Public-key and attribute certificate frameworks, 2001년 5월, ITU-T

[2] IETF RFC2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile

[3] IETF RFC2511 Internet X.509 Certificate Request Message Format

[4] IETF Draft Internet X.509 Public Key Infrastructure Permanent Identifier

[5] 식별번호를 이용한 본인확인 기술규격, 2002년 9월, 한국정보보호진흥원

[6] X9.62, The Elliptic Curve Digital Signature Algorithm (ECDSA), 1999년 1월, ANSI

[7] WAP-217-WPKI Version 24-Apr-2001 Wireless Application Protocol Public Key Infrastructure Definition

[8] Y. Zheng. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature)+cost (encryption). In: CRYPTO'97, LNCS 1294, pp.165-179. Springer Verlag, 1997.

[9] Y. Zheng. Signcryption and its application in efficient public key solutions. In: Information Security Workshop (ISW '97), LNCS 1396, pp. 291-312. Springer-Verlag, 1997.

[10] F. Bao and R. H. Deng. A signcryption scheme with signature directly verifiable by public key. In: Public Key Cryptography(PKC'98), LNCS 1431, pp.55-59, Springer-Verlag, 1998.

[11] Guilin Wang, Feng Bao, Changshe Ma, and Kefei Chen. Efficient Authenticated Encryption Schemes with Public Verifiability. In: Proc. of the 60th IEEE Vehicular Technology Conference (VTC 2004-Fall) - Wireless Technologies for Global Security. IEEE Computer Society, 2004.

김 성 덕

e-mail : sdkim@koscom.co.kr

1994년 성균관대학교 정보공학과(학사)

1996년 성균관대학교 정보통신대학원 (석사)

2004년 성균관대학교 정보통신대학원 박사수료

1996년~1999년 한국전산원 초고속사업단

1999년~현재 한국증권전산 시스템사업본부(공인인증센터)

관심분야 : PKI, 무선통신 보안, 전자문서 보관소

정 재 동

e-mail : jjd@koscom.co.kr

1983년 연세대학교 수학과(학사)

1994년 연세대학교 산업대학원(석사)

2002년 숭실대학교 대학원 공학박사

1982년~현재 한국증권전산 시스템사업본부장

관심분야 : S/W엔지니어링, PKI, 암호학, 정보보안, 전자상거래 등

원 동 호

e-mail : dhwon@dosan.skku.ac.kr

성균관대학교 전자공학과(학사, 석사, 박사)

1978년~1980년 한국전자통신연구원 전임연구원

1985년~1986년 일본 동경공업대 객원 연구원

1988년~1999년 성균관대학교 교학처장, 전기전자 및 컴퓨터 공학부장, 정보통신대학원장, 정보통신기술연구소장

1996년~1998년 국무총리실 정보화추진위원회 자문위원

2002년~2003년 한국정보보호학회장

2003년~2004년 성균관대학교 연구처장

1982년~현재 성균관대학교 정보통신공학부 교수, 정보통신부 지정 정보보호인증기술연구센터장

관심분야 : 암호 프로토콜, 정보 보안 등