Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.2, Apr. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.2.293

복수 K-FIDO 기기 환경에서의 인증키 관리

이 병 천†‡
중부대학교

Certified Key Management in Multi K-FIDO Device Environment

Byoungcheon Lee†‡
Joongbu University

요 약

생체인식 기술을 이용하여 기존의 패스워드를 대체하기 위한 FIDO(Fast IDentity Online)[1,7] 기술이 빠르게 성장하고 있다. FIDO 기술은 생체인식 기술을 이용한 편리한 사용자 인증과 스마트카드 기술을 이용한 안전한 키관리 기능을 제공하지만 사용자 신원인증 기술이 함께 제공되지 않아 사용자가 FIDO 기기를 원격 서버에 초기 등록하는 과정에서는 기존의 전통적인 신원인증 방식을 이용할 수밖에 없다. K-FIDO[3]는 이런 단점을 해결하기 위하여 FIDO 기술과 인증서기반 기술을 하나의 기기에 접목시킨 것으로 사용자의 초기등록 과정에서 인증서 기반 인증을 이용할 수 있게 하였다. 그런데 사용자들이 복수의 K-FIDO 기기를 사용하는 유비쿼터스 환경이 빠르게 도래할 것으로 예상되는데, 이런 환경에서는 만일 기존의 방식대로 하나의 인증서를 여러 기기에 복사하여 사용하거나, 기기별로 별도의 인증서를 발급받아 사용하게 된다면 많은 문제가 발생할 것으로 예상된다. 본 논문에서는 자체확장인증[4] 방식을 이용하여 복수 K-FIDO 기기 환경에서 인증키 관리의 편의성을 향상시킬 수 있는 방안을 제시한다.

ABSTRACT

FIDO(Fast IDentity Online) technology is expanding very rapidly which can replace traditional password-based authentication with biometrics technology[1,7]. FIDO provides convenient authentication with biometrics technology and secure key management with smart card technology, but it does not provide user identification, thus traditional user identification technology should be used before a FIDO device is registered to a FIDO server. K-FIDO[3] is an approach to implement FIDO and certificate-based authentication technology into a single device that user can utilize certificate-based authentication in initial registration of FIDO device to FIDO server. It is expected that very shortly users will own and use multiple K-FIDO devices. If we consider the traditional approach of copying single certificate to multiple devices or issuing independent certificate to each device, there will be many complex problems. In this paper we propose more secure and convenient key management technology in multiple K-FIDO device scenario using self-extended certification[4].

Keywords: FIDO, K-FIDO, multi-device key management, self-extended certification

I. 서 론

컴퓨터와 인터넷을 이용한 IT세계에서 안전한 서비스를 제공하기 위해서는 사용자의 신원을 확인하는 인증기술이 가장 선결되어야 할 기반기술이다. 패스워드는 고대로부터 사용된 기본적인 인증방식인데 고도화된 정보화 시대로 발전한 오늘날에서도 여전히 널리 사용되고 있다. 패스워드는 도청공격, 사전공격 등 여러 가지 공격에 취약점이 있어서 사용을 중지해야 한다는 주장이 커지고 있지만 아직까지도 널리 사용되고 있는데 그 이유는 그동안 편의성 및 구현의 간편성 측면에서 패스워드를 대체할 수 있는 뚜렷한

Received(02. 17. 2017.), Modified(03. 28. 2017), Accepted(03. 29. 2017)
† 주저자, sultan@joongbu.ac.kr
‡ 교신저자, sultan@joongbu.ac.kr(Corresponding author)

대체기술이 없었기 때문이다.

패스워드를 대체할 수 있는 보다 근본적인 인증기술로서 FIDO(Fast IDentity Online)[1,7] 기술이 등장하였고 최근 빠르게 발전하고 있다. 이것은 사용자 소유의 로컬기기에 대한 사용자 인증을 위해 생체인식 등 편리한 인증기술을 사용하고 있고 로컬기기와 원격 서버와는 전자서명 기반의 안전한 인증을 사용하는데, 이 두가지 기술이 안전하고 편리하게 결합되어 있어서 사용자의 인증 편의성을 크게 높이고 있다. 즉, 사용자는 자신이 소유한 로컬기기에 생체인증으로 접근을 허가받으면 원격지 서버에의 전자서명 인증도 한번에 수행되는 것이다.

그런데 FIDO 기술은 패스워드를 대체할 수 있는 생체인증 기술과 스마트카드 기술에 기반한 안전한 키관리 및 전자서명 기반의 인증 기능을 제공하고 있지만 사용자의 신원을 확인하기 위한 인증체계는 함께 제공하지 않고 있다. 그러므로 사용자가 FIDO 기기를 원격 서버에 초기 등록하는 경우에는 기존에 사용하던 패스워드를 이용한 인증, 주민등록번호 등의 식별번호 제시, SMS등 통신사 기반의 인증, 계좌정보/신용카드정보 등 금융사 기반의 인증, 공인인증서를 이용한 인증 등 별도의 전통적인 인증방식으로 사용자의 신원을 확인한 이후에야, FIDO 기기에서 새로운 키쌍을 생성하고 FIDO 서버에 공개키를 등록하게 된다. 같은 FIDO 기기를 또다른 원격 서버에 등록하기 위해서는 이러한 불편한 신원확인 방식을 반복해야 하기 때문에 사용자 편의성 측면에서 문제가 있다.

한국에서 개발되고 있는 K-FIDO[3] 기술은 FIDO모듈과 인증서 관련 모듈을 하나의 기기에 함께 내장한 것으로, K-FIDO기기에 한번 인증서를 발급받으면 원격 서버에 대한 초기 등록시에 인증서 기반의 명시적 인증을 사용할 수 있어서 사용자 편의성을 크게 높일 수 있다. 이것은 한국이 선도적으로 발전시켜온 공인인증기술에 FIDO기반의 안전하고 편리한 인증수단을 활용하기 위한 노력이라고 볼 수 있다.

그런데 향후 관련 산업이 발전하고 FIDO 기술의 적용이 확대되면 사용자들이 복수개의 K-FIDO 기기를 사용하게 되는 유비쿼터스 환경으로 빠르게 발전할 것으로 예상된다. 예를 들면, FIDO 인증기능을 내장한 스마트폰, FIDO 지문인식 신용카드, 웨어러블 기기, TPM(Trusted Platform Module)형 FIDO 모듈을 내장한 컴퓨터 등 많은 K-FIDO 기기들을 사용하게 될 것이다. 이 경우 한 사용자가 자신이 소유하는 복수개의 K-FIDO 기기에 인증서를 발급/설치하여 사용하려고 하면 다음과 같은 세가지 방법을 이용할 수 있을 것인데 이들은 복잡한 문제를 야기하게 된다.

첫째, 하나의 K-FIDO 기기에 인증서를 발급받고 이를 다른 기기로 복사하여 사용하는 방법은 보안성 측면에서 바람직하지 않고 이런 방식으로 사용하려면 스마트카드 기반의 안전한 키관리 기능을 사용하지 못하게 된다. 스마트카드 기술은 내부에서 키쌍을 생성하고 개인키를 외부로 복사해낼 수 없는 안전영역에 저장할 수 있도록 되어 있는데 이러한 표준기술을 사용할 경우 개인키를 외부로 복사할 수 있는 방법이 없기 때문이다.

두 번째 방법으로 복수개의 K-FIDO 기기별로 별도의 인증서를 발급받아 사용하는 방법이 있을 수 있는데, 이것은 개인이 인증서 발급 및 안전한 관리에 기기의 수만큼 간여해야 하므로 많은 복잡성을 야기하게 된다. 사용자에게 인증서를 발급하기 위해서는 엄밀한 신분확인이 중요한데 이것을 기기의 수만큼 반복하는 것은 사용자 및 인증기관에게 매우 번거로운 일이 될 것이다. 더구나 사용자는 기기의 수가 많아질수록 이들 모두를 안전하게 관리하기 어렵다는 근본적인 한계가 있으며, 기기를 분실하게 되면 인증서를 폐기해야 하는데 인증기관 측면에서는 인증서 폐기를 관리하는 것도 큰 부담이 될 것이다.

세 번째 방법으로 기기별로 인증서를 발급하지 않고 하나의 마스터기기에만 인증서를 발급받고 다른 기기들의 사용시에는 마스터기기로 인증을 푸시하여 사용하는 방법이 있다. FIDO에서 제시하는 CTAP(Client to Authenticator Protocol)[2] 방식은 사용자가 항상 소지하게 되는 스마트폰 등 하나의 마스터기기를 별도의 인증장치로 사용하는 방식으로 다른 기기에서 인증 필요시 마스터기기로의 2채널 인증을 확인하도록 하는 방식이다. 이 방법은 인증서가 저장된 하나의 기기만 안전하게 관리하면 되므로 키관리가 편리하다는 장점도 있지만 인증시 마스터기기와의 온라인 통신이 필수적이며, 사용자의 활동을 하나의 마스터기기로 제약하는 결과를 낳게 되어 마스터기기가 없으면 모든 활동이 중단되는 단점이 있다. 특히 사물인터넷 환경에서와 같이 사용자의 개입 없이 복수의 기기들이 자동으로 인증된 통신을 하고자 하는 경우에는 기기별로 별도의 인증키를 가질 필요가 있는데 이런 경우에는 적용하기 어렵다.

또한 인증서를 클라우드에 저장하고 인증 필요시마다 클라우드 서비스를 호출하여 사용하는 방식이 있을 수 있는데 이 방식은 개인키가 클라우드에 저장됨으로 인해 클라우드 보안이 매우 중요해지고 클라우드에 저장된 개인키를 사용하는 권한을 확인하기 위해서는 현재 사용중인 기기와 클라우드 서버와의 또다른 인증이 필요하게 된다는 단점이 있다.

향후 유비쿼터스 환경으로 발전하면서 많은 컴퓨팅 기기들에 TEE(Trusted Execution Environment), SE(Secure Element), TPM(Trusted Platform Module) 등으로 불리우는 하드웨어보안모듈들이 기본 내장되는 환경으로 발전할 것으로 예상되는데 이런 내재적 보안환경을 적극 사용할 수 있는 방안이 제시되어야 한다. 사용자가 사용하는 모든 기기들에 인증키를 안전하게 내장하여 사용자들이 보안에 신경을 쓰지 않아도 안전성이 보장되는 내재적 보안을 제공하는 것이 중요할 것이다.

자체확장인증[4] 기술은 한 사용자가 복수개의 컴퓨팅기기를 사용하는 환경에서 인증키 관리의 편의성을 제공하기 위해 제안된 기술로, 사용자가 인증서를 발급받은 하나의 마스터기기를 이용하여 자신이 소유하는 추가기기들에 자체확장인증서를 발행하여 사용할 수 있도록 하는 기술이다. 여기서 자체확장인증서란 사용자 추가기기에서 생성된 키쌍에 대해 사용자의 인증서로 서명한 별도의 인증서로서 사용자가 마스터기기를 이용하여 스스로 발행하는 것이다. 마스터기기와 추가기기 간의 자체확장인증서 발행을 위한 통신을 효율적으로 중개하기 위해 별도로 운영되는 키관리서버를 이용하는 자체확장인증서 발급 모델도 제시되었다[5].

한편 ID기반 암호와 인증서기반 암호를 결합 활용하여 추가기기들에 자체확장 ID개인키를 발급하여 사용하는 방식도 제안되어 있다[6]. 이것은 사용자의 마스터기기는 인증기관이 발급하는 인증서를 가지고 있지만 추가기기의 인증은 마스터기기가 발행하는 ID개인키를 사용하도록 하는 방식으로 사용자의 추가기기들이 인증서 대신 공개할 수 있는 ID정보를 공개키로 사용할 수 있도록 하여 키관리의 편의성을 크게 높일 수 있다.

이 논문에서는 사용자들이 복수의 K-FIDO 기기들을 사용하게 되는 환경에서 인증서를 가지고 있는 하나의 K-FIDO 마스터기기를 이용하여 복수개의 추가 K-FIDO 기기들에 인증서를 배포하기 위한 편리한 기술을 제안하고 있는데, 사용자 스스로 자체확장인증서를 발행하여 사용하는 기술과 함께 사용자의 인증서를 이용한 명시적인 발급요청이 있는 경우 인증기관이 추가기기에게 추가인증서를 자동 발급하도록 운영하는 방안을 제시한다. 또한 ID기반 암호를 결합 활용하는 방식에서는 ID개인키 발행을 안전하고 편리하게 구현하는 방안에 대해서 검토한다.

II. 관련 연구

2.1 FIDO

FIDO 얼라이언스[1]는 2012년에 설립된 글로벌 인증 관련 기업들의 연합체로 인증기술에 대한 기술표준을 제시하고 관련 산업을 확산시키는 것을 목표로 한다. 2014년에 FIDO 1.0 표준이 발표되었으며 2015년에 FIDO 2.0 표준이 발표되었다.

FIDO 표준은 두가지 인증 프로토콜을 제시하고 있다. 첫 번째는 패스워드 없는 인증을 위한 UAF (Universal Authentication Protocol)로 사용자 기기에서 생체인증 기술 등으로 사용자를 검증하면 전자서명을 이용하는 원격서버와의 인증을 자동으로 수행하도록 하는 기술이다. 두 번째는 U2F (Universal 2nd Factor)로 기존에 널리 사용되는 패스워드 기반의 온라인 인증 시스템에서 두 번째 인증요소로 FIDO 디바이스를 제시하도록 요구하는 방식이다. FIDO 얼라이언스는 FIDO 기술을 웹서비스 인증에도 적용하기 위해 W3C에 표준안을 제출하고 있다[9].

FIDO 기술은 로컬 인증수단과 원격 인증 프로토콜을 분리하여 구현하되 FIDO 디바이스에서 사용자가 검증되면 원격서버와의 인증을 자동 수행하도록 운영하여 보안과 사용자 편의성을 향상시켰다. 로컬 인증수단이 원격 인증 프로토콜과 독립되어 있으므로 지문, 홍채, 얼굴인식, 패스워드 등 다양한 인증수단을 손쉽게 적용할 수 있다.

그런데 FIDO 기술에서는 사용자 신원 확인을 위한 인증체계는 함께 제공하고 있지 않다. FIDO 얼라이언스에서는 기기의 초기 등록시 인증수단(Authenticator)과 사용자의 신원을 연결하는 것은 FIDO 표준 밖의 일이라고 선언하고 있다. 사용자 신원확인을 위해서는 이미 사용하고 있는 전통적인 신원인증 방식을 이용해야 할 것인데, 패스워드 기반 인증, 주민등록번호 등의 개인식별번호 제시, SMS등 통신사 기반의 인증, 계좌정보/신용카드정보

등 금융사 기반의 인증, 공인인증서를 이용한 인증 등 복잡한 신원인증 방식을 이용하게 될 것이다. FIDO에서는 인증수단 등록시 사용자의 신원이 확인된 이후 인증수단에서 새로운 키쌍을 생성하여 개인키는 내부에 안전하게 저장하고 공개키를 서버에 등록하게 된다. FIDO에서는 원격 서버별로 서로 다른 키쌍을 등록하여 사용하기 때문에 사용자의 프라이버시(privacy), 비연결성(non-linkability)을 제공할 수 있다는 장점이 있다. 그러나 같은 FIDO 기기를 여러 곳의 원격 서버에 등록하여 사용하기 위해서는 이러한 불편한 신원확인 방식을 반복해야 하기 때문에 사용자 편의성 측면에서 문제가 있다.

2.2 K-FIDO

한국에서는 사용자 신원인증의 안전성과 편의성을 높이기 위해 2000년 전자서명법이 시행된 이후 공인인증 기술을 도입하여 사용해 왔다. 공인인증서는 사용자의 신원과 사용자가 사용하는 공개키에 대해 공인인증기관이 서명하여 발급하는 문서로 이들간의 위조할 수 없는 명시적인 결합을 제공하고 있다. 그러므로 별도의 추가적인 신분확인이 필요없이 공인인증서의 검증만으로 사용자의 신분을 확인할 수 있기 때문에 많은 서비스들의 사용자 인증에 손쉽게 적용할 수 있다는 확장성에 큰 장점이 있다.

그런데 한국에서 적용되어 온 공인인증기술은 안전한 키관리 수단이 부족한 상태에서 사용됨으로 인해 많은 금융사고를 겪어왔다. 즉 사용자의 개인키를 사용자가 입력하는 패스워드로 암호화하여 PC의 하드디스크에 저장하여 사용하는 방식을 사용해왔는데, 사용자가 선택하는 패스워드는 복잡도가 높지 않고, 동일한 패스워드를 여러 다른 서비스에도 사용하는 경향이 있으며, 키로깅 등의 해킹으로 패스워드를 쉽게 탈취당할 수 있다. FIDO에서 사용하는 생체인증 기반의 인증수단은 패스워드에 의존할 필요 없는 스마트카드 기술 기반의 안전한 키관리 수단이라는 측면에서 큰 장점이 있으며 이를 현재의 공인인증체계와 결합하여 안전한 키관리 수단으로 사용하려는 노력은 당연한 시도라고 하겠다.

2016년 KISA를 중심으로 바이오 공인인증 서비스라는 이름으로 개발된 K-FIDO[3] 기술은 FIDO 모듈과 공인인증 모듈을 하나의 기기에 구현하여 공인인증서의 개인키를 FIDO 기기 내에 저장하고 개인키 암호화 비밀번호를 입력해야 했던 것을 FIDO 생체인식으로 대체할 수 있도록 한 것이다. 즉 개인키를 사용하기 위해서는 패스워드를 입력할 필요가 없이 생체인증만 하면 전자서명이 수행될 수 있도록 구현하였다.

FIDO 기기와 같은 스마트카드 기반의 기술에서는 키쌍을 스마트카드 내부에서 생성하고 개인키는 외부로 빼낼 수 없는 안전한 저장소에 저장하고 개인키를 사용하는 연산도 기기 내부에서 수행하도록 하고 있다. 스마트카드의 운영체제에는 개인키를 외부로 추출하기 위한 기능 자체를 제공하지 않고 있어서 스마트카드는 인증서와 개인키를 안전하게 저장할 수 있는 가장 근본적인 인증수단이라고 볼 수 있다.

그런데 현재의 K-FIDO 기술에서는 PC에서 사용해왔던 패스워드 기반 암호화 기술을 여전히 사용하고 있다. 즉 사용자가 생체인증으로 신원을 검증하면 K-FIDO 기기는 디바이스 고유의 내부정보나 사용자 생체정보 등을 기반으로 패스워드를 자동 생성하게 되며 이를 이용하여 개인키를 암호화하여 저장하도록 하고 있다. 전자서명 등 개인키를 사용하는 연산을 하기 위해서는 동일한 정보를 기반으로 패스워드를 계산한 후에 암호화된 개인키를 복호화하여 개인키를 추출한 후 사용하게 된다. 또한 같은 과정을 거쳐 개인키를 외부로 복사해낼 수 있고 다른 기기로 복사하여 사용할 수 있도록 하고 있다.

개인키를 이런 방식으로 관리하는 것은 스마트카드 고유의 안전한 키관리 기술을 사용하지 않고 있다는 것을 의미한다. K-FIDO에서 이런 변형된 개인키 관리 방식을 채용한 것은 사용자가 복수의 기기들을 사용하게 되고 이들 기기에 동일한 인증서를 복사하여 사용할 수 있도록 서비스해야 할 필요성이 있어서 어쩔 수 없이 사용하는 것으로 생각된다.

그러나 패스워드로 암호화하는 개인키 저장 방식은 PC 환경에서 경험한 바와 같이 많은 취약성을 가지고 있다. 설사 FIDO 기기 내부에서는 안전하게 저장된다고 가정하더라도 암호화된 개인키를 외부로 복사하는 경우 통신상으로 전달되는 암호화된 개인키 파일은 공격자의 주된 공격목표가 될 수 있다. FIDO 기술에서는 개인키를 패스워드가 필요없이 안전하게 관리하고 있는데 K-FIDO로 공인인증 기능을 추가하면서 안전하지 않은 키관리 방식으로 변형하여 사용하고 있는 것이다.

2.3 자체확장인증

한 사용자가 복수의 컴퓨팅기기를 사용하는 환경에서의 인증서 발급/설치/관리의 편의성을 높이기 위해 자체확장인증 기술이 제안되었다[4,5,6]. 이것은 사용자가 인증기관으로부터 발급받은 하나의 인증서를 기반으로 자신이 소유한 복수기기에 자체확장인증서를 스스로 발행하여 사용하는 방법론이다[4]. 자체확장인증서란 사용자의 기기에서 키쌍을 생성하고 그 공개키에 대해 동일 사용자의 인증서로 서명하여 생성하는 인증서를 말한다.

사용자는 복수의 컴퓨팅기기를 사용하고 있으며 이들 기기에는 스마트카드 기술 기반의 안전한 하드웨어 보안모듈을 장착하고 있다고 가정한다. 사용자가 인증기관으로부터 인증서를 발급받은 하나의 기기를 마스터기기라고 하며 나머지 기기들을 추가기기라고 부르자. 사용자는 추가기기들에도 인증키를 설치하여 사용하고자 한다. 마스터기기가 자체확장인증서를 발급하는 기능을 갖춘 키관리서버의 기능을 가지고 있다면 통신을 통해 추가기기들에 자체확장인증서를 발급해 줄 수 있다[4].

그런데 개인이 자신만을 위한 키관리서버를 소유하고 운영하는 것은 경제적인 부담도 크고 안전하게 운영하기가 쉽지 않아서 매우 부담스러운 일이 아닐 수 없다. 이를 해결하기 위해 자체확장인증서 발급을 중개하는 기능을 갖춘 전용 키관리서버를 전문회사가 운영하도록 하고, 사용자들은 클라이언트 입장에서 키관리서버에 접속하여 1) 추가기기를 이용하여 자체확장인증서 발급 신청을 하고, 2) 마스터기기를 이용하여 자체확장인증서를 발행하고 이것을 키관리서버에 저장하도록 하며, 3) 추가기기에서 자체확장인증서를 다운로드 받아 사용하는 방식이 제안되었다[5]. 이런 방법을 이용하면 하나의 키관리서버가 많은 사용자들에게 자체확장인증서 발행을 중개하는 서비스를 제공할 수 있고 사용자별 자체확장인증서 발행내역을 관리할 수도 있게 된다.

2.4 ID기반 암호를 이용한 자체확장인증

ID기반 암호와 인증서기반 암호를 결합 사용하여 자체확장인증을 구현하는 방식이 [6]에 제안되었다. ID기반 암호[8]는 사용자가 선택하는 ID, 이메일주소 등의 공개할 수 있는 평문정보를 사용자의 공개키로 사용할 수 있게 하는 암호기술로, 공개키와 쌍이 되는 개인키는 별도의 개인키생성기관(Private Key Generator, PKG)이 계산하여 사용자에게 비밀채널을 통해 안전하게 전달해 주어야 한다. ID기반 암호는 인증서가 필요없이 공개할 수 있는 임의의 정보를 공개키로 사용할 수 있어서 인증키의 배포 측면에서 많은 장점이 있다.

그러나 ID기반 암호의 사용을 주저하게 만드는 요인 중의 하나는 사용자의 개인키를 스스로 생성하는 것이 아니라 PKG라는 남이 만들어 준다는 것이다. 그러므로 PKG에 대한 전적인 신뢰가 전제되어야 사용할 수 있다.

자체확장인증 시나리오에 ID기반 암호를 적용하면 인증서를 발급받은 마스터기기가 PKG의 역할을 하여 추가기기에 ID개인키를 발급하도록 하면 되는데, 이 경우 ID개인키를 사용하게 되는 추가기기나 ID개인키를 발급해주는 마스터기기(PKG)가 동일 사용자 소유이기 때문에 서로 신뢰할 수 있어서 위에서와 같은 문제가 발생하지 않는다. 이런 측면에서 인증서 기반 암호와 ID기반 암호를 결합 사용하는 방식은 자체확장인증 환경에 적용 가능한 최적의 암호시스템이라고 볼 수 있다.

위 논문에서는 인증서를 장착하고 있는 마스터기기가 추가기기에서 사용할 ID개인키를 생성하여 주입하는 방식의 프로토콜을 제시하였다. ID개인키는 추가기기의 ID 정보를 인증서의 개인키로 서명한 것이며 ID개인키를 이용한 서명의 검증시에는 인증서의 공개키를 함께 사용해야 하므로 사용자의 신분을 자연스럽게 확인할 수 있게 된다.

III. 복수 K-FIDO 기기 환경의 인증키 관리

사용자가 복수의 K-FIDO 기기를 소유하고 있다고 가정하고 인증서 기반의 인증키를 안전하게 배포하기 위한 방안을 생각해보자. K-FIDO 기기에서 제공하는 스마트카드 기반의 안전한 키관리 기능을 적극 활용할 수 있는 방안을 우선 고려한다.

여기에서는 하나의 K-FIDO 기반 마스터기기에 인증서를 발급받아 장착하고 있는 환경에서 나머지 복수의 K-FIDO 기반 추가기기들에게 자체확장인증 방식으로 인증키를 발급하는 방식을 자세히 설명한다. 첫 번째 방식은 사용자가 키관리서버를 통신 중개매체로 이용하여 직접 자체확장인증서를 발행하여 사용하는 방법이고, 두 번째 방식은 인증기관이 추가인증서 발급의 주체가 되는 방식으로 사용자의 명시

적인 추가인증서 발급요구가 제시된 경우(즉 기존의 인증서로 서명된 추가인증서 발급요구가 있는 경우) 인증기관이 추가인증서를 자동 발급하도록 운영하는 방식이다. 세 번째 방식은 ID기반 암호를 결합 사용하는 경우 키관리서버를 중개로 하여 ID개인키를 안전하게 전달하는 방식이다.

3.1 사용자에 의한 자체확장인증서 발급

여기에서는 외부의 전문기관이 운영하는 자체확장인증서 발급을 중개하는 역할을 하는 키관리서버(key management server, KMS)를 사용할 수 있다고 가정한다. 사용자는 인증기관(certificate authority, CA)으로부터 인증서(certificate)를 발급받아 장착하고 있는 하나의 마스터기기(master device)를 가지고 있고 복수개의 추가기기(additional device)에 자체확장인증서(self-extended certificate, SEC)를 발급하여 사용하려고 한다. 먼저 사용자는 마스터기기를 이용하여 키관리서버에 계정을 등록하고 인증서를 등록하여야 한다. 이후 사용자가 추가기기와 마스터기기를 이용하여 자체확장인증서를 발급하는 과정은 다음과 같으며 이를 Fig. 1에 도시하였다.

(1) 자체확장인증서 발급 요청 (추가기기)

사용자는 추가기기를 이용하여 키관리서버에 접속하고 자체확장인증서 발급을 요청한다. 이때 추가기기에서는 키쌍을 생성하여 개인키는 K-FIDO 기기의 안전영역에 보관하고 공개키와, 기기명, 사용자 정보를 개인키로 서명하여 발급요청서를 생성하여 키관리서버에 전송한다. 여기에서 기기명은 복수의 추가기기를 구분하기 위한 용도의 정보이다. 이때 사용자에게 참조정보를 제공하기 위해 발급요청 내역에 대한 해쉬값을 화면에 출력할 수 있다.

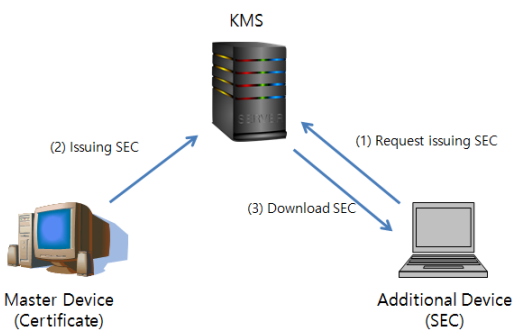

Fig. 1. Issuing SEC by user

(2) 자체확장인증서 발급 (마스터기기)

사용자는 마스터기기를 이용하여 키관리서버에 접속하고 발급요청 내역을 검색하여 화면에 출력되는 해쉬값을 비교한다. 자신이 추가기기로 요청했던 내역이 검색되면 발급 버튼을 누른다. 이때 마스터기기 내에 저장된 개인키로 서명하여 자체확장인증서가 생성되며 이것이 키관리서버로 전송된다. 키관리서버는 수신한 자체확장인증서를 사용자 계정에 추가 저장한다.

(3) 자체확장인증서 다운로드 (추가기기)

사용자는 추가기기를 이용하여 키관리서버에 접속하고 자체확장인증서 발급내역을 검색하여 존재하는 경우 자체확장인증서를 다운로드한다.

키관리서버는 사용자의 계정정보와 함께 사용자의 자체확장인증서 발행 내역을 안전하게 관리하여야 하며, 사용자는 키관리서버에 로그인하여 자신의 자체확장인증서 발행 내역을 언제든지 검색해 볼 수 있어야 한다. 필요한 경우 키관리서버는 타인에게도 사용자의 자체확장인증서 발행내역의 정보를 제공할 수 있다.

이러한 키관리서버의 동작은 단순한 통신 중개자의 역할이므로 관리자의 간여가 필요없이 자동적으로 운영하도록 할 수 있다. 사용자의 추가기기를 이용한 자체확장인증서 발급요청, 마스터기기를 이용한 자체확장인증서 발급 등에 대한 내역이 서명된 정보로 존재하므로 사용자의 책임이 명확하다. 자체확장인증서 발급 여부에 대한 분쟁 발생시 키관리서버는 이러한 서명된 정보를 증거로 제시할 수 있다.

자동화된 서비스로 운영하는 키관리서버는 사용자 인증에 대한 부담이 적기 때문에 더 많은 사용자들을 대상으로 자체확장인증서 발급 중개 서비스를 제공할 수 있다. 예를 들어 인증서를 발급해준 인증기관이 서로 다른 사용자들도 동일한 키관리서버를 이용할 수 있다.

3.2 인증기관에 의한 추가인증서 자동 발급

위에서 제시된 모델은 자체확장인증서 발행을 중개하기 위한 별도의 키관리서버의 존재를 가정하고 있는데 이러한 서비스는 사용자에게 인증서를 발급해

준 해당 인증기관(certificate authority, CA)이 사용자에 대한 추가서비스의 하나로 직접 제공할 수도 있다. 즉, 추가인증서 발급요청에 대해 사용자의 인증서로 서명된 명시적인 동의가 있는 경우 인증기관은 별도의 사용자 신분인증과정을 거치지 않고 추가인증서(additional certificate, AC)를 자동 발급하도록 운영하는 것이다. 사용자는 인증서를 발급받은 하나의 마스터기기(master device)를 가지고 있으며 복수의 추가기기(additional device)에 인증키를 발급하여 사용하려고 한다. 사용자의 마스터기기 인증서는 이미 인증기관에 등록되어 있음을 고려하자. 인증기관을 이용한 추가인증서(additional certificate, AC) 자동 발급 과정은 다음과 같으며 이를 Fig. 2에 도시하였다.

(1) 추가인증서 발급 요청 (추가기기)

사용자는 추가기기를 이용하여 인증기관에 접속하고 추가인증서 발급을 요청한다. 이때 추가기기에서는 키쌍을 생성하여 개인키는 K-FIDO 기기의 안전영역에 보관하고 공개키와, 기기명, 사용자 정보를 개인키로 서명하여 발급요청서를 생성하여 키관리서버에 전송한다. 이때 사용자에게 참조정보를 제공하기 위해 발급요청 내역에 대한 해쉬값을 화면에 출력할 수 있다.

(2) 추가인증서 발급 동의 (마스터기기)

사용자는 마스터기기를 이용하여 인증기관에 접속하고 추가인증서 발급요청 내역을 검색하여 화면에 출력되는 해쉬값을 비교한다. 자신이 추가기기로 요청했던 내역이 검색되면 발급 동의 버튼을 누른다. 이때 마스터기기 내에 저장된 개인키로 서명한 발급동의서가 생성되며 인증기관에 전송된다.

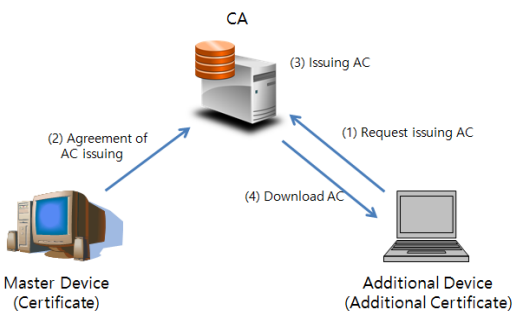

Fig. 2. Automatic issuing of additional certificate by CA

(3) 추가인증서 자동 발급 (인증기관)

인증기관은 사용자의 인증서로 서명된 발급동의서가 제출되면 서명을 검증한 후 추가인증서를 자동 발급하여 자신의 DB에 저장한다.

(4) 추가인증서 다운로드 (추가기기)

사용자는 추가기기를 이용하여 인증기관에 접속하고 추가인증서 발급내역을 검색하여 존재하는 경우 추가인증서를 다운로드한다.

이렇게 발급되는 추가인증서는 인증기관이 새로 발급하는 것이지만 마스터기기에 이미 발급된 인증서와 논리적으로 밀접하게 연결된 인증서이다. 추가인증서의 유효기간은 마스터기기에 발급된 사용자 인증서와 동일하게 설정하고 마스터기기 인증서 정보를 확장영역에 기록하여 원래의 사용자 인증서와 연계된 추가인증서임을 제시할 수 있다.

일반적으로 인증기관이 사용자에게 인증서를 발급하는 과정에서는 사용자의 신분에 대한 엄밀한 검증이 필요하며 여기에 많은 비용이 소요된다. 그러나 기존에 발급된 인증서를 이용한 사용자의 명시적인 동의가 제시된 경우 별도의 사용자 신분 검증을 생략하고 추가인증서를 자동 발급하도록 운영하는 것이다. 만일 이렇게 발급된 추가인증서가 잘못 이용되는 경우 인증기관은 사용자의 귀책사유를 증명할 수 있게 된다. 인증기관이 이러한 추가서비스를 제공한다면 복수 K-FIDO 기기 환경에서도 인증서를 안전하게 배포하고 관리할 수 있다.

3.3 ID기반 자체확장인증키 발급

현재의 FIDO 기기에는 타원곡선 암호의 하나인 ECDSA가 구현되어 있으므로 타원곡선 암호로 구현되는 ID기반 암호를 적용하려는 노력이 가능한 단계에 있다. 그러므로 인증서 기반 암호와 ID기반 암호를 결합 활용하는 자체확장인증은 FIDO기기에 적용하기에 매우 적합한 키관리 모델이라고 볼 수 있다.

우선 [6]에 제시된 인증서 발급 및 ID개인키 발행 과정을 간단히 살펴보자.

(1) 인증서 발급 (인증기관 ↔ 마스터기기)

인증기관은 키쌍 (s_0, P_0)을 가지고 있으며 여기서 $P_0 = s_0 P$이다. 사용자 A는 마스터기기에서

$P_A = s_A P$의 관계를 갖는 키쌍 (s_A, P_A)을 생성한다. 사용자 A는 인증기관에게 공개키 P_A를 전송하며 인증서 발급을 요청한다. 인증기관은 A에게 인증서 $Cert_A$를 다음과 같이 생성하여 전송한다.

$$Cert_A = s_0 H(CI_A, P_A)$$

여기서 CI_A는 인증서 양식에 포함되는 사용자 정보를 나타낸 것으로 공개키 P_A와 함께 인증기관이 서명하여 인증서를 생성한다. 인증서를 발급받은 사용자 A는 인증서의 유효성을 다음과 같이 검증할 수 있다.

$$e(Cert_A, P) = e(H(CI_A, P_A), P_0)$$

(2) ID개인키 발급 (마스터기기 → 추가기기)

인증서에 표시된 사용자의 이름이 A이고 추가기기의 이름을 M이라고 하자. 추가기기가 사용할 ID 공개키는 $Q_{A.M} = H(A, M)$이고 ID개인키는 $D_{A.M} = s_A Q_{A.M}$이다. 마스터기기는 추가기기에 $D_{A.M}$을 안전하게 전달하여야 한다. 추가기기는 자신이 전달받은 ID개인키의 유효성을 다음과 같이 검증할 수 있다.

$$e(D_{A.M}, P) = e(H(A, M), P_A)$$

이렇게 발급된 ID개인키는 전자서명, 공개키암호화, 키분배 등에 널리 사용될 수 있다[6].

이 모델에서 사용자는 인증서가 발급된 하나의 마스터기기를 가지고 있고 복수의 추가기기들에 ID개인키를 발행하여 사용하려고 한다. ID개인키는 마스터기기가 생성하며 이것을 추가기기들에 안전하게 전달하여야 한다. 앞에서 설명한 자체확장인증서는 공개될 수 있는 정보이므로 공개적인 통신을 통해 전달하여도 문제가 없었지만 ID개인키는 개인의 신원을 증명하는데 사용하는 기밀 정보이므로 공격자에게 노출되지 않도록 안전하게 전달되어야 한다. 이러한 ID개인키의 안전한 발급 측면에서 가능한 구현 방법에 대해 검토해보자.

(1) 로컬 통신을 통해 직접 ID개인키를 전달

마스터기기와 추가기기에 ID개인키를 생성하고 로컬통신을 통해 전달하는 기능이 구현되어 있는 경우 ID개인키는 마스터기기로부터 추가기기로 직접 전달될 수 있다. 로컬통신을 통해 직접 전달하면 온라인 통신을 모니터링하고 있는 네트워크 공격자의 공격을 피할 수 있을 것이다. 이러한 기능은 전용 앱으로 구현하거나 운영체제의 기본기능으로 구현될 수 있다.

(2) 키관리서버를 통한 암호화된 ID개인키 전달

마스터기기와 추가기기 사이의 통신을 중개하는 키관리서버가 있다고 가정하자. 사용자는 마스터기기를 이용하여 추가기기에서 사용할 ID개인키를 생성하고 안전한 패스워드를 이용하여 암호화 후 키관리서버에 전송한다. 사용자는 추가기기를 이용하여 키관리서버에 접속하고 암호화된 ID개인키를 다운로드하고 동일한 암호를 입력하여 ID개인키를 복호화하고 추가기기에 설치한다. 여기서 키관리서버는 통신중개수단으로서의 역할만 수행하게 되며 ID개인키에 대한 정보를 얻을 수 없다.

이 이외에도 ID개인키를 안전하게 전달하는 것은 여러 가지 방법이 가능할 것이며 안전하면서도 사용자 편의성이 높게 구현되어야 할 것이다. ID개인키는 추가기기 내부에서 생성된 것이 아니라 마스터기기에서 생성하여 추가기기에 주입하여 사용하는 방식이므로 스마트카드의 안전영역에 저장하고 사용하는 방식에 대한 설계가 필요하다.

IV. 분 석

이 논문에서 제시된 사용자가 스스로 발행하여 사용하는 자체확장인증서, 인증기관이 자동 발행하는 추가인증서 방식은 다음과 같은 특징이 있다.

1) 스마트카드 기술 기반의 안전한 키의 활용

사용자가 스마트카드 기술 기반의 복수 K-FIDO 기기를 사용하는 경우 기기 내부에서 안전하게 생성/이용/보관되는 키쌍을 인증키로 활용할 수 있는 효율적인 방법론을 제시하였다.

2) 사용자 영역내의 계층적 인증키 관리

자체확장인증서, 추가인증서는 마스터기기 인증서

에서 파생된 인증서이며 이들의 유효성 검증시에는 마스터기기 인증서가 필요하다. 마스터기기 인증서가 폐기되거나 갱신되는 경우에는 기존 발행한 자체확장 인증서, 추가인증서가 무효화되므로 다시 생성하여 사용해야 한다. 이들의 사용에 문제가 있을 경우에는 언제든지 다시 발행하여 사용할 수 있다. 추가기기의 분실 등으로 기존의 인증키들을 무효화하고자 하는 경우에는 마스터기기 인증서를 갱신하면 된다.

3) 인증키의 사용자 직접 관리

사용자가 복수의 기기를 사용하고 있다면 이것의 구입, 폐기, 매도 등 관리주체는 사용자이다. 그런데 기기마다 인증키의 발급/폐기 등을 위하여 외부의 인증기관에 여러번 의존해야 한다는 것은 논리적으로 맞지 않으며 문제 해결에 어려움을 겪게 될 수 있다. 자체확장인증서, 추가인증서 모델은 사용자가 직접 인증키를 관리하는 모델이며 발행 내역을 언제든지 확인할 수 있어서 안전한 관리가 가능하다.

4) 인증키 관리를 위한 키관리서비스의 활용

사용자가 다수의 컴퓨팅기기, 온라인 서비스 들에 패스워드 기반 인증을 사용하는 경우 패스워드 관리에 어려움을 겪고 있는 이유는 패스워드가 개인이 보관해야 할 기밀정보이며 남에게 위탁하기 어렵다는 특징 때문이다. 그러므로 패스워드를 관리하는 것은 전적으로 개인의 책임으로 외부 서비스의 도움을 받기가 쉽지 않다. 그러나 인증서는 공개될 수 있는 정보이며 인증서 발급과정도 공개된 통신채널로 수행할 수 있다. 위에서 제시한 바와 같이 자체확장인증서, 추가인증서 발행 과정에서 키관리서버와 인증기관의 도움을 받을 수 있으며 발행내역이 언제든지 확인 가능하도록 관리되고 있다. 개인 사용자는 외부의 키관리서비스의 도움을 받아 자신 영역내의 복수 K-FIDO 기기들에 인증키 관리를 편리하게 수행할 수 있게 되었다.

V. 결 론

FIDO 인증기술은 패스워드에 대한 의존성을 근본적으로 해결할 수 있는 안전하고 편리한 인증수단으로서 빠르게 확산될 것으로 보인다. K-FIDO는 한국에서 사용되어온 공인인증체계에 FIDO의 안전하고 편리한 인증수단을 결합하여 기존의 공인인증체계에서 경험해 온 개인키 저장방식의 취약점을 해결하고자 하는 시도이다.

우리가 당면한 또다른 도전과제는 사용자가 복수의 K-FIDO 기기들을 사용하는 환경에서의 안전한 인증서 배포 및 관리 문제이다. 기존의 PC환경에서나 현재의 K-FIDO에서 도입하고 있는 하나의 인증서를 여러 기기에 복사하여 사용하는 방식과 이를 가능하게 하기 위한 개인키의 패스워드 암호화 저장 방식은 임시 방편으로 사용해 온 것이며 보다 근본적인 해결방안을 제공해야 한다. 이런 측면에서 이 논문에서 제시한 자체확장인증 방식은 사용자 스스로 자체확장인증서를 발행하여 사용하거나, 인증기관이 추가인증서를 자동 발행하는 방식으로 위의 문제점들을 해결할 수 있다. 이러한 접근방법은 사용자의 K-FIDO 기기 내부에서 생성되는 안전한 키쌍을 인증키로 사용할 수 있게 하여 내재적인 보안을 제공해 준다. 더구나 사용자의 자체확장인증서 및 추가인증서 발행 내역을 키관리서버 및 인증기관에서 안전하게 관리할 수 있는 방법론을 제공하고 있다.

ID기반 암호화를 적용한 자체확장인증 방식은 인증서 대신 ID 등의 공개정보를 공개키로 이용할 수 있는 방식으로 인증키 배포 및 관리가 편리한 장점이 있다. 특히 K-FIDO 기기에서는 타원곡선 암호를 사용할 수 있는 환경이 제공되므로 인증서 기반 암호와 ID기반 암호를 결합 활용하는 자체확장인증 방식의 적용을 시도해볼 수 있다. 사용자들이 편리하게 사용할 수 있도록 하는 키관리 방식의 상세한 구현 방안에 대해서는 좀 더 연구가 필요하다.

인증서의 복사 활용 대신에 CTAP와 같이 복수의 기기에서 인증시 하나의 마스터기기를 인증수단으로 사용하는 방식도 이용되고 있는데 이것이 편리한 경우도 있지만 모든 경우에 적합한 것은 아니다. 이 방법은 인증서가 저장된 하나의 기기만 안전하게 관리하면 되므로 키관리가 편리하다는 장점도 있지만 인증시 마스터기기와의 온라인 통신이 필수적이며, 사용자의 활동을 하나의 마스터기기로 제약하는 결과를 낳게 되어 마스터기기가 없으면 모든 활동이 중단되는 단점이 있다. 특히 사물인터넷 환경에서와 같이 사용자의 개입 없이 복수의 기기들이 자동으로 인증된 통신을 하고자 하는 경우에는 기기별로 별도의 인증키를 가질 필요가 있는데 이런 경우에는 적용하기 어렵다. 그러므로 CTAP 방식과 자체확장인증서 방식은 서로 대립된 기술이 아니라 필요에 따라 병행하여 사용될 수 있는 기술이다.

자체확장인증서를 발행하여 사용하는 것이 현재로

서는 복잡해 보일지 모르지만 사용자가 새로운 기기를 구입하는 경우 수행해야 하는 환경설정의 하나로 생각하면 크게 부담스러운 것은 아니다. 사용자가 새로운 기기를 구입한 경우 기본적으로 접근제어 패스워드 설정 등 환경설정 과정을 거치고 사용을 시작하게 되는데 현재로서는 사용자의 소유권을 등록하는 명시적인 멤버십 등록과정이 없다. 이의 개선 방안으로 마스터기기를 이용하여 새로운 기기의 멤버십을 등록하게 하고 이 과정에서 자체확장인증서를 설치하여 사용하게 하면 새로운 기기는 하나의 사용자 인증서에 결합된 명시적인 멤버십을 가지게 된다. 이러한 환경설정 과정을 거치면 사용자 기기는 전자상거래 등 사용자 신분을 이용한 거래에 즉시 사용될 수 있는 환경을 갖추게 된다.

복수 K-FIDO 기기 환경에서의 안전한 키관리 문제는 유비쿼터스 환경으로 발전해 나가는 상황에서 우리가 당면한 도전과제로서 이를 해결하기 위한 보다 적극적인 노력이 필요하다고 생각된다. 자체확장 인증 기술은 표준 공개키기반구조(PKI) 체계의 기술을 일부 변형하여 적용한 것으로 현재의 표준기술이 아니라는 비판이 있을 수 있지만, 오히려 기존의 표준기술이 해결하지 못해온 이런 도전과제를 해결할 수 있는 새로운 접근방법이라고 생각할 수 있다. 또한 이 기술을 표준기술로 추가하기 위한 표준화 노력과 함께 필요한 세부 구현기술을 개발하는 선도적인 노력을 기울일 필요가 있다. 이 논문에서는 가장 기본적인 키관리 방식을 제안한 것이며 이를 실제 구현하고 서비스화하기 위해서는 전문기업에 의한 많은 추가 연구개발이 필요하다고 생각된다.

References

〔1〕 FIDO alliance, https://fidoalliance.org/

〔2〕 R. Lindermann, V. Bharadwaj, A. Czeskis, and M.B. Jones, "FIDO 2.0: Client To Authenticator Protocol," Oct. 2016, https://fidoalliance.org/specs/fido-v2.0-rd-20161004/fido-client-to-authenticator-protocol-v2.0-rd-20161004.html

〔3〕 KISA, "Implementation Guideline for Safe Usage of Accredited Certificate using bio information in Smart phone," KCAC.TG.IMP, 2016. 9.

〔4〕 Byoungcheon Lee, "Hybrid Key Management Using Self-Extended Certification and Hardware Security Module," Journal of Security Engineering, 11(4), pp. 273-286, Aug. 2014.

〔5〕 Byoungcheon Lee, "Model of Key Management Server for Hybrid Certification," Journal of Security Engineering, 13(1), pp. 27-40, Feb. 2016.

〔6〕 Byoungcheon Lee, "Hybrid-Style Personal Key Management in Ubiquitous Computing," Proceedings of the 11th International Conference on Security and Cryptography (SECRYPT2014), pp. 238-243, Aug. 2014.

〔7〕 S.R. Cho, D.S. Choi, S.H. Jin, and H.H. Lee, "Passwordless Authentication Technology - FIDO," Electronics and Telecommunications Trends, 29(4), pp. 101-109. Aug. 2014.

〔8〕 D. Boneh, and M. Franklin, "Identity-based encryption from the Weil pairing," Advances in Cryptology - Crypto'2001, LNCS 2139, pp. 213 - 229. SpringerVerlag. Aug. 2001.

〔9〕 H.L.V. Gong, D. Balfanz, A. Czeskis, A. Birgisson, and J. Hodges, "FIDO 2.0: Web API for accessing FIDO 2.0 credentials," Nov. 2015, https://www.w3.org/Submission/2015/SUBM-fido-web-api-20151120/

〈저자소개〉

이 병 천 (Byoungcheon Lee) 종신회원
1986년 2월: 서울대학교 물리학과 학사
1988년 2월: 서울대학교 물리학과 석사
2002년 2월: KAIST 정보보호 박사
2002년 3월~현재: 중부대학교 정보보호학과 교수
〈관심분야〉 정보보호, 암호, 인증, 네트워크보안, 웹보안, IoT보안