通信情報保護學會誌
第5卷 第1號, 1995. 3

ISO/IEC JTC1/SC27의 국제표준소개 (7) : ISO/IEC IS9798_3 정보기술 - 보안기술 - 실체인증 기법, 제 3 부: 공개키 알고리듬을 이용한 인증

(Information technology - Security techniques - Entity authentication mechanisms - Part 3: Entity authentication using a public key algorithm)

이 필 중*

요 약

지난 호에 이어 상대방이 자신이라고 주장한 실체가 정말 그 실체인지를 인증하기 위한 기법을 표준화하는 과제 중의 세번째로 "공개키 알고리듬을 이용한 인증"을 소개한다. 이 과제는 1990년 CD(Committee Draft), 1992년 DIS(Draft for International Standard)가 되었고, 1993년에 IS(International Standard)가 되었으며 1998년에 1차 검토가 있을 예정이다.

1. 범 위 〔Scope〕

ISO/IEC 9798의 제 3 부에서는 공개키 알고리듬을 사용한 실체인증 기법을 기술한다. 그 중 두 가지 기법은 한 쪽의 실체만 인증하는 일방인증에 관한 것이고 나머지는 두 실체의 상호인증에 관한 기법이다. 실체의 신분 검증에는 디지탈 서명을 사용한다. 이때 신뢰성 있는 제 3 자를 포함할 수도 있다. 〔This part of ISO/IEC 9798 specifies entity authentication mechanisms using a public key algorithms. Two mechanisms are concerned with the authentication of a single entity(unilateral authentication) while the remaining are mechanisms for mutual authentication of two entities. A digital signature is used to verify the identity of an entity. A trusted third party may be involved.〕

ISO/IEC 9798의 제 3부에서 기술되는 기법들은 한번 사용된 유효한 인증 정보가 재사용되는 것을 막기 위해 시각표, 일련번호, 난수값과 같은 시간변이 변수를 사용한다. 〔The mechanisms specified in this part of ISO/IEC 9798 use time variant parameters such as time stamps, sequence numbers, or random numbers, to prevent valid authentication information from being accepted at a later time.〕

* 포항공과대학교 전자전기공학과

시각표나 일련번호를 사용할 때는 1회 전송만으로 일방인증을 할 수 있지만, 상호인증에는 적어도 2회의 전송이 필요하다. 난수값을 사용한 시도-응답 방법일 때는, 일방인증에 2회의 전송이 필요하고, 상호인증에는 (채용한 기법에 따라) 3회 내지 4회의 전송이 필요하다. [If a time stamp or a sequence number is used, one pass is needed for unilateral authentication, while two passes are needed to achieve mutual authentication. If a challenge and response method employing random numbers is used, two passes are needed for unilateral authentication, while three or four passes (depending on the mechanism employed) are required to achieve mutual authentication.]

2. 참고문헌 [Normative reference]

아래의 표준 ISO/IEC 9798의 제 1부는 본문의 참고문헌으로서 ISO/IEC 9798의 제 3 부를 구성하는 규정들을 포함하고 있다. 본 표준은 발표 당시에는 유효했다. 모든 표준은 개정되기 마련이므로 ISO/IEC 9798의 제 3부를 근거로 삼으려는 사람들은 아래에 명시한 표준의 최신 개정본을 찾아 보기 바란다. IEC와 ISO의 회원들이 최신 국제 표준을 관리한다.

[The following standard contains provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 9798. At the time of publication, the edition indicated was valid. All standards are subject to revision, and parties to agreements based on this part of ISO/IEC 9798 are encouraged to investigate the possibility of applying the most recent edition of the standard indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.]

ISO/IEC 9798-1: 1991, Information technology - Security techniques - Entity authentication mechanisms - Part 1: General model.

3. 정의와 표기법 [Definitions and notation]

ISO/IEC 9798 제 3 부에는 ISO/IEC 9798 제 1부에서 기술한 정의와 표기법을 적용한다.

[For the purposes of this part of ISO/IEC 9798 the definitions and notation described in ISO/IEC 9798-1 apply.]

4. 요구조건 [Requirements]

ISO/IEC 9798 제 3 부에 기술하는 인증 기법은 인증되어야 할 실체가 비밀 서명키를 알고 있음을 보여줌으로써 자신의 실체를 증명하는 것이다. 인증되어야 할 실체는 비밀 서명키로 특정한 데이터를 서명한다. 그러면 이 실체의 공개 검증키를 사용하는 어느 누구라도 서명을 검증할 수 있다. [In the authentication mechanisms specified in this part of ISO/IEC 9798 an entity to be authenticated corroborates its identity by demonstrating its knowledge of its secret signature key. This is achieved by the entity using its secret signature key to sign specific data. The signature can be verified by anyone using the entity's public verification key.]

위의 인증 기법에는 다음과 같은 요구조건이 있다. 이들 중에 하나라도 충족되지 않으면 인증 절차를 손상시키거나 이행할 수 없게 된다. [The authentication mechanisms have the

following requirements. If any of these is not met then the authentication process may be compromised or it cannot be implemented.〕

a) 검증자에게는 주장자의 유효한 공개키가 있어야 한다. 〔a) A verifier shall possess the valid public key of the claimant.〕

b) 주장자에게는 자신만이 알고 있고 사용할 수 있는 비밀 서명키가 있어야 한다. 〔b) A claimant shall have a secret signature key known and used only by itself.〕

주 인증서를 이용하는 것이 유효한 공개키를 얻는 한가지 방법이다(부록 B 참조). 그러나 인증서의 생성, 분배, 폐기는 ISO/IEC 9798 제 3부의 범위를 벗어나는 것이다. 또다른 방법으로 신뢰성 있는 제 3자가 개입할 수도 있다. 그밖에 신뢰성 있는 전령을 개입시키는 방법도 있다. 〔Note - One way of obtaining a valid public key is by means of a certificate(see annex B). The generation, distribution, and revocation of certifcates are outside the scope of this part of ISO/IEC 9798. There may exist a trusted third party for this purpose. Another way of obtaining a valid public key is by trusted courier.〕

5. 인증 기법 〔Mechanisms〕

기술하는 실체인증 기법들은 시각표, 일련번호, 난수값과 같은 시간변이 변수를 사용한다(부록 C 참조). 〔The specified entity authentication mechanisms make use of time variant parameters such as time stamps, sequence numbers or random numbers(see annex C).〕

ISO/IEC 9798 제 3 부에서는 다음과 같이 토큰을 정의한다.

$$\text{Token} = X_1 \| \cdots \| X_i \| sS_A (Y_i \| \cdots \| Y_j)$$

"서명한 데이터"는 서명에 대한 입력으로 사용하는 "$Y_i \| \cdots \| Y_j$"를 가리키며 "서명하지 않은 데이터"는 "$X_1 \| \cdots \| X_i$"를 가리킨다. 〔In this part of ISO/IEC 9798, given a token defined as

$$\text{Token} = X_1 \| \cdots \| X_i \| sS_A (Y_i \| \cdots \| Y_j)$$

the "signed data" refers to "$Y_i \| \cdots \| Y_j$" used as input to the signature scheme and the "unsigned data" refers to "$X_1 \| \cdots \| X_i$".〕

토큰의 서명한 데이터에 있는 정보를 서명에서 복구할 수 있으면 토큰의 서명하지 않은 데이터에는 이 정보를 포함시키지 않아도 된다(ISO/IEC 9796을 예로 참조). 〔If information contained in the signed data of the token can be recovered from the signature, then it need not be contained in the unsigned data of the token(see, for example, ISO/IEC 9796).〕

토큰의 서명한 데이터에 있는 정보(예를 들면, 난수값)를 검증자가 이미 알고 있으면, 주장자가 보낸 토큰의 서명하지 않은 데이터에는 이 정보를 포함시키지 않아도 된다. 〔If information in the signed data of the token (e. g., a random number) is already known to the verifier, then it need not be contained in the unsigned data of the token sent by the claimant.〕

아래의 인증 기법들에서 기술하는 모든 텍스트 필드의 응용은 ISO/IEC 9798 제 3부의 범위를 넘어선다(공란으로 둘 수도 있다). 텍스트 필드의 내용과 텍스트 필드간의 관계는 어떻게 응용하느

냐에 달려 있다. 텍스트 필드의 사용법에 대한 정보는 부록 A에 있다. [All text fields specified in the following mechanisms are available for use in applications outside the scope of this part of ISO/IEC 9798 (they may be empty). Their relationship and contents depend upon the specific application. See annex A for information on the use of text fields.]

㈜ 인증서의 분배는 ISO/IEC 9798 제 3부의 범위 밖이므로, 모든 인증 기법에서 인증서를 보내는 것은 선택 사항이다. [NOTE - As the distribution of certificates is outside the scope of this part of ISO/IEC 9798, the sending of certificates is optional in all mechanisms.]

5.1 일방인증 [Unilateral authentication]

일방인증이란 인증 기법을 사용하여 두 실체중 한 쪽만을 인증하는 것을 의미한다. [Unilateral authentication means that only one of the two entities is authenticated by use of the mechanism.]

5.1.1 1회 전송 인증 [One pass authentication]

이 인증 기법은 주장자 A가 인증 절차를 시작하고 주장자 A를 검증자 B가 인증한다. 시각표나 일련번호를 생성시키고 이를 조사함으로써 고유성 / 적시성을 통제한다(부록 C 참조). [In this authentication mechanism the claimant A initiates the process and is authenticated by the verifier B. Uniqueness / timeliness is controlled by generating and checking a time stamp or a sequence number(see annex C).]

1회 전송 인증 기법을 그림 1에 나타내었다. [The authentication mechanism is illustrated in figure 1.]

그림 1

주장자 A가 검증자 B에게 보내는 토큰(Token AB)의 형식은 다음과 같다. [The form of the token (TokenAB), sent by the claimant A to the verifier B is:]

$$\text{TokenAB} = \begin{matrix} T_A \\ N_A \end{matrix} \| B \| \text{Text2} \| sS_A(\begin{matrix} T_A \\ N_A \end{matrix} \| B \| \text{Text1}),$$

이때 주장자 A는 시간변이 변수로 일련번호 N_A나 시각표 T_A를 사용한다. 시간변이 변수는 주장자와 검증자의 기술적 역량과 인증이 이루어지는 환경에 따라 선택한다. [where the claimant A uses either a sequence number N_A or a time stamp T_A as the time variant parameter. The choice depends on the technical capabilities of the claimant and the verifier as well as on the environment.]

㈜1 목표한 검증자 이외의 실체가 토큰을 받아들이는 것을 막기 위하여 실체명 B를 Token AB의 서명한 데이터에 포함시켜야 한다. [The inclusion of the identifier B in the signed data of TokenAB is necessary to prevent the token from being accepted by anyone other than the intended verifier.]

㈜2 일반적으로 텍스트2는 이 인증 절차에서 인증되지 않는다. [In general, Text2 is not authenticated by this process.]

주3 이 인증 기법의 한 가지 응용으로 키분배가 있다(부록 A 참조). [One application of this mechanism could be key distribution(see annex A).]

(1) *A*는 *B*에게 TokenAB를 보내는데, 인증서를 보내는 것은 선택 사항이다. [*A* sends TokenAB and, optionally, its certificate to *B*.]

(2) TokenAB가 있는 메시지를 받으면 *B*는 다음의 과정을 수행한다. [On receipt of the message containing TokenAB, *B* performs the following steps:]

(i) *A*의 인증서를 검증하거나 그 밖의 방법으로 메시지가 *A*의 유효한 공개키를 갖고 있음을 확인한다. [It ensures that it is in possession of a valid public key of *A* either by verifying the certificate of *A* or by some other means.]

(ii) 시각표나 일련번호를 조사하고 토큰에 있는 *A*의 서명을 검증한 뒤, TokenAB의 서명한 데이터에 있는 실체명 필드(B)의 값이 실체 *B*의 고유 실체명과 같은지를 조사함으로써 TokenAB를 검증한다. [It verifies TokenAB by checking the time stamp or the sequence number, by verifying the signature of *A* contained in the token and by checking that the value of the identifier field (*B*) in the signed data of TokenAB is equal to entity B's distinguishing identifier.]

5.1.2 2회 전송 인증 [Two pass authentication]

이 인증 기법은 검증자 *B*가 인증 절차를 시작하여 주장자 *A*를 인증한다. 난수값 R_B를 생성시키고 이를 조사함으로써 고유성 / 적시성을 통제한다(부록 C 참조). [In this authentication mechanism the claimant A is authenticated by the verifier B who initiates the process. Uniqueness / timeliness is controlled by generating and checking a random number RB(see annex C).]

2회 전송 인증 기법을 그림 2에 나타내었다. [The authentication mechanism is illustrated in figure 2.]

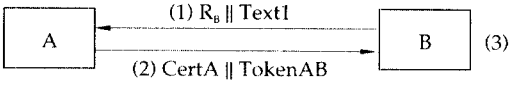

그림 2

주장자 *A*가 검증자 *B*에게 보내는 토큰(Token AB)의 형식은 다음과 같다. [The form of the token (TokenAB), sent by the claimant *A* to the verifier *B* is:]

$$\text{TokenAB} = R_A \| R_B \| B \| \text{Text3} \| sS_A(R_A \| R_B \| B \| \text{Text2}).$$

TokenAB에서 변수 *B*의 포함 여부는 선택 사항으로 이 인증 기법이 이용되는 환경에 달려있다. [The inclusion of the parameter *B* in TokenAB is optional. It depends on the environment in which this authentication mechanism used.]

주 인증 기법을 시작하기에 앞서 *B*가 자신이 선택한 데이터 상에 대한 *A*의 서명을 얻는 것을 막기 위해 TokenAB에는 난수값 R_A가 있다. 예를 들어, *A*가 동일한 키를 실체 인증 이외의 목적으로도 사용할 경우에 이러한 예방 조치가 필요하다. [NOTE - The random number R_A is present in TokenAB to

prevent B from obtaining the signature of A on data chosen by B prior to the start of the authentication mechanism. This prevention may be required, for example, when the same key is used by A for other purposes in addition to entity authentication.〕

(1) B는 난수값 R_B를 보내는데, 텍스트 필드 Text1을 A에 보내는 것은 선택 사항이다. 〔B sends a random number R_B and, optionally, a text field Text1 to A.〕

(2) A는 B에게 TokenAB를 보내는데, 인증서를 보내는 것은 선택 사항이다. 〔A sends Token AB and, optionally, its certificate to B〕

(3) TokenAB가 있는 메시지를 받았을 때, B는 다음의 과정을 수행한다. 〔On receipt of the message containing TokenAB, B performs the following steps:〕

(i) A의 인증서를 검증하거나 그 밖의 방법으로 A의 유효한 공개키를 갖고 있음을 확인한다. 〔It ensures that it is in possession of a valid public key of A either by verifying the certificate of A or by some other means.〕

(ii 토큰에 있는 A의 서명을 검증하고, 과정 (1)에서 A에게 보내진 난수값 R_B가 TokenAB의 서명한 데이터에 있는 난수값과 같은지를 조사함으로써 TokenAB를 검증한다. 〔It verifies TokenAB by checking the signature of A contained in the token and by checking that the random number R_B, sent to A in step (1), agrees with the random number contained in the signed data of TokenAB.〕

5.2 상호인증 〔Mutual authentication〕

상호인증이란 인증기법을 사용하여 두 통신 실체가 서로를 인증하는 것을 의미한다. 〔Mutual authentication means that the two communicating entities are authenticated to each other by use of the mechanism.〕

상호인증을 하기 위해 5.1.1과 5.1.2에서 기술한 두 기법들이 5.2.1과 5.2.2에서 각각 확장된다. 여기서는 메시지를 하나 더 보내기 때문에 두 개의 과정이 추가된다. 〔The two mechanisms described in 5.1.1 and 5.1.2 are extended in 5.2.1 and 5.2.2 respectively, to achieve mutual authentication. This is done by transmitting one further message resulting in two additional steps.〕

5.2.3에서 기술하는 기법은 네 개의 메시지를 사용하는데 네 개를 모두 연속으로 보내지 않아도 된다. 이런 방법으로 인증 절차를 가속화한다. 〔The mechanisms specified in 5.2.3 uses four massages which, however, need not all be sent consecutively. In this way the authentication process may be speeded up.〕

5.2.1 2회 전송 인증 〔Two pass authentication〕

이 인증 기법은 시각표나 일련번호를 생성시키고 이를 조사함으로써 고유성 / 적시성을 통제한다(부록 C 참조). 〔In this authentication mechanism uniqueness / timeliness is controlled by generating and checking time stamps or sequence numbers(see annex C).〕

2회 전송 인증 기법을 그림 3에 나타내었다.

[The authentication mechanism is illustrated in figure 3.]

그림 3

A가 B에게 보내는 토큰(TokenAB)의 형식은 5.1.1에서 기술한 것과 동일하다. [The form of the token (TokenAB), sent by A to B, is identical to that specified in 5.1.1.]

$$\text{TokenAB} = {}^{T_A}_{N_A} \| B \| \text{Text2} \| sS_A({}^{T_A}_{N_A} \| B \| \text{Text1}).$$

B가 A에게 보내는 토큰(TokenBA)의 형식은 다음과 같다. [The form of the token (TokenBA), sent by B to A, is:]

$$\text{TokenAB} = {}^{T_B}_{N_B} \| A \| \text{Text4} \| sS_B({}^{T_B}_{N_B} \| A \| \text{Text3})$$

이 기법에서 시각표와 일련번호 중 어느 것을 사용할지는 주장자와 검증자의 기술적 역량과 인증이 이루어지는 환경에 달려 있다. [The choice of using either time stamps or sequence numbers in this mechanism depends on the technical capabilities of the claimant and the verifier as well as on the environment.]

주1 예정된 검증자 이외의 실체가 토큰을 받아들이는 것을 막기 위하여 실체명 A와 B를 TokenBA와 TokenAB의 서명한 데이터에 각각 포함시켜야 한다. [NOTE 1 - The inclusion of identifiers A and B in the signed data of TokenBA and TokenAB, respectively, is necessary to prevent the tokens from being accepted by anyone other than the intended verifier.]

과정 (1)과 (2)는 5.1.1에서 기술한 것과 동일하다. [Steps (1) and (2) are identical to those specified in 5.1.1, one pass authentication.]

(3) B는 A에게 TokenBA를 보내는데 인증서를 보내는 것은 선택 사항이다. [B sends TokenBA and, optionally, its certificate to A.]

(4) 과정 (3)의 메시지는 5.1.1의 과정 (2)와 유사한 방법으로 다룬다. [The message in step (3) is handled in a manner analogous step (2) of 5.1.1.]

주2 이 기법의 두 메시지는 적시성 이외에는 어떤 식으로도 서로 결부되어 있지 않다. 이 기법에서는 5.1.1의 기법을 독립적으로 두 번 사용한다. 이 메시지들을 더욱 결부시키고자 한다면 텍스트 필드를 적절히 사용할 수 있다 (부록 A 참조). [NOTE 2 - The two messages of this mechanism are not bound together in any way, other than implicitly by timeliness; the mechanism involves independent use of mechanism 5.1.1 twice. If it is desired to bind these messages further, appropriate use could be made of text fields(see annex A).]

5.2.2 3회 전송 인증 [Three pass authentication]

이 인증 기법은 난수값을 생성시키고 이를 조사함으로써 고유성 / 적시성을 통제한다(부록 C 참조). [In this authentication mechanism uniqueness / timeliness is controlled by generating and checking random numbers(see annex C).]

3회 전송 인증 기법을 그림 4에 나타내었다. 〔The authentication mechanism is illustrated in figure 4.〕

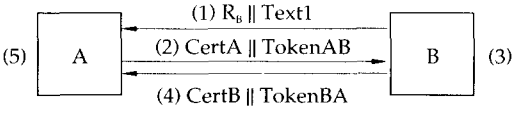

그림 4

토큰의 형식은 다음과 같다. 〔The tokens are of the following form:〕

$$\text{TokenAB} = R_A \| R_B \| B \| \text{Text3} \| sS_A(R_A \| R_B \| B \| \text{Text2}),$$

$$\text{TokenBA} = R_B \| R_A \| A \| \text{Text5} \| sS_B(R_B \| R_A \| A \| \text{Text4}).$$

TokenAB에서 변수 B의 포함 여부와 TokenBA에서 변수 A의 포함 여부는 선택 사항으로 이 인증 기법이 이용되는 환경에 달려 있다. 〔The inclusion of the parameter B in TokenAB and the inclusion of the parameter A in TokenBA are optional. They depend on the environment in which this authentication mechanism is used.〕

㈜ 인증 기법을 시작하기에 앞서 B가 자신이 선택한 데이터에 대한 A의 서명을 얻는 것을 막기 위해 TokenAB에는 난수값 R_A가 있다. 예를 들어, A가 동일한 키를 실체 인증 이외의 목적으로도 사용할 경우에 이러한 예방 조치가 필요하다. 유사한 이유로 난수값 R_B가 TokenBA에 있다. 나아가 이 난수값이 첫번째 메시지의 난수값과 같은지를 확인하는 것이 보안상의 이유로 꼭 필요하다. 〔NOTE - The random number R_A is present in TokenAB to prevent B from obtaining the signature of A on data chosen by B prior to the start of the authentication mechanism. This prevention may be required, for example, when the same key is used by A for other purposes in addition to entity authentication. For similar reasons the random number R_B is present in TokenBA. Furthermore checking that this random number is the same as the random number in the first message is necessary for security considerations.〕

(1) B는 A에게 난수값 R_B를 보내는데 텍스트 필드 Text1을 보내는 것은 선택 사항이다. 〔B sends a random number R_B and, optionally, a text field Text1 to A.〕

(2) A는 B에게 TokenAB를 보내는데 인증서를 보내는 것은 선택 사항이다. 〔A sends Token AB and, optionally, its certificate to B.〕

(3) TokenAB가 있는 메시지를 받았을 때, B는 다음의 과정을 수행한다. 〔On receipt of the message containing TokenAB, B performs the following steps:〕

(i) A의 인증서를 검증하거나 그 밖의 방법으로 A의 유효한 공개키를 갖고 있음을 확인한다. 〔It ensures that it is in possession of a valid public key of A either by verifying the certificate of A or by some other means.〕

(ii) 토큰에 있는 A의 서명을 검증하고, 과정 (1)에서 A에게 보내진 난수값 R_B가 TokenAB의 서명한 데이터에 있는 난수값과 같은지를 조사함으로써 TokenAB를 검증한다. 〔It verifies TokenAB by checking the signature of A contained in the token and by checking that the

random number R_B, sent to A in step (1), agrees with the random number contained in the signed data of TokenAB.〕

(4) B는 A에게 TokenBA를 보내는데 인증서를 보내는 것은 선택 사항이다. 〔B sends Token BA and, optionally, its certificate to A.〕

(5) TokenBA가 있는 메시지를 받았을 때, A는 (3)의 과정 (i)과 (ii)를 유사한 과정을 수행한다. 그밖에 A는 TokenBA의 서명한 데이터에 있는 난수값 R_B가 과정 (1)에서 받은 난수값 R_B와 같은지를 확인한다. 〔On receipt of the message containing TokenBA, A analogously performs steps (i) and (ii) listed under (3). In addition, A checks that the random number R_B contained in the signed data of TokenBA is equal to the random number R_B received in step (1).〕

5.2.3 2회 전송 병렬 인증 〔Two pass parallel authentication〕

이 기법에서는 인증을 병렬적으로 수행한다. 고유성 / 적시성은 난수값을 생성시키고 조사함으로써 통제한다(부록 C 참조). 〔In this mechanism authentication is carried out in parallel. Uniqueness/timeliness is controlled by generating and checking random numbers(see annex C).〕

2회 전송 병렬 인증 기법을 그림 5에 나타내었다. 〔The authentication mechanism is illustrated in figure 5.〕

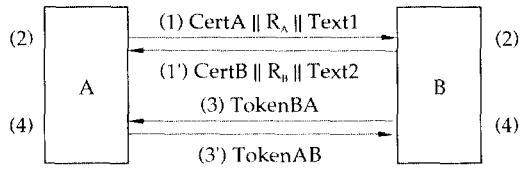

그림 5

토큰의 형식은 5.1.2항에 나와 있는 것과 유사하다. 〔The tokens are similar to those of clause 5.1.2:〕

$$\text{TokenAB} = R_A \| R_B \| B \| \text{Text4} \| sS_A(R_A \| R_B \| B \| \text{Text3}),$$

$$\text{TokenBA} = R_B \| R_A \| A \| \text{Text5} \| sS_B(R_B \| R_A \| A \| \text{Text4}).$$

TokenAB에서 변수 B의 포함 여부와 TokenBA에서 변수 A의 포함 여부는 선택 사항으로 이 인증 기법이 이용되는 환경에 달려 있다. 〔The inclusion of the parameter B in TokenAB and the inclusion of the parameter A in TokenBA are optional. They depend on the environment in which this authentication mechanism is used.〕

㈜1 인증 기법을 시작하기에 앞서 B가 자신이 선택한 데이터에 대한 A의 서명을 얻는 것을 막기 위해 TokenAB에는 난수값 R_A가 있다. 예를 들어, A가 동일한 키를 실체 인증 이외의 목적으로도 사용할 경우에 이러한 예방 조치가 필요하다. 유사한 이유로 난수값 R_B가 TokenBA에 있다. 〔NOTE 1 - The random number R_A is present in TokenAB to prevent B from obtaining the signature of A on data chosen by B prior to the start of the authentication mechanism. This prevention may be required, for example, when the same key is used by A for other purposes in addition to entity authentication. For

similar reasons the random number R_B is present in TokenBA.〕

(1) A는 B에게 난수값 R_A를 보내는데, 인증서와 텍스트 필드 Text1을 보내는 것은 선택 사항이다. 〔A sends a random number R_A and, optionally, a text field Text1 to B.〕

(1′) B는 A에게 난수값 R_B를 보내는데, 인증서와 텍스트 필드 Text2를 보내는 것은 선택 사항이다. 〔B sends R_B and, optionally, its certificate and a text field Text2 to A.〕

(2) A와 B는 각자의 인증서를 검증하거나 그 밖의 방법으로 상대 실체가 유효한 공개키를 갖고 있음을 확인한다. 〔A and B ensure that they are in possession of a valid public key of the other entity either by verifying the respective certificate or by some other means.〕

(3) B는 A에게 TokenBA를 보낸다. 〔B sends TokenBA to A.〕

(3′) A는 B에게 TokenAB를 보낸다. 〔A sends TokenAB to B.〕

(4) A와 B는 다음의 과정을 수행한다. 〔A and B perform the following steps:〕

A와 B 각자는 토큰에 있는 서명을 확인하고 상대방 실체에게 이전에 보낸 난수값과 과정 (3) 및 (3′)에서 받은 토큰의 서명한 데이터에 있는 난수값이 일치하는지를 확인함으로써 과정 (3) 및 (3′)에서 받은 토큰을 검증한다. 〔Each of them verifies the received token by checking the signature contained in the token and by checking that the random number, which it previously sent to the other entity, agrees with the random number contained in the signed data of the token received.〕

주2 5.2.3의 기법에 대한 또다른 한가지 방법은 5.1.2의 기법을 양방향으로 수행하는 것이다. 5.2.3에서 첫번째 메시지에 인증서를 포함시키면 빨리 인증서를 검증할 수 있어서 인증 절차를 가속화한다. 〔NOTE 2 - An alternative to mechanism 5.2.3 is to run mechanism 5.1.2 both ways. The inclusion of the certificates in the first messages of mechanism 5.2.3 allows for earlier certificate verification which may speed up the authentication process.〕

부록 A 〔Annex A〕
(참고) (informative)
텍스트 필드의 사용
〔Use of text fields〕

ISO/IEC 9798의 제 3부의 5절에서 규정한 토큰들은 텍스트 필드를 포함한다. 토큰의 전송에서 다양한 텍스트 필드들의 관계와 실제적인 사용은 응용하기에 달려 있다. 예들을 살펴보면 다음과 같다. 만약 메시지 복원형 디지탈 서명이 사용되지 않고 텍스트 필드가 사용되었다면, 검증자는 서명을 확인하기 전에 텍스트를 알고 있어야 한다. 이 부록에서 "서명한 텍스트 필드"는 서명한 데이터에 포함된 텍스트 필드를 말하며 "서명하지 않은 텍스트 필드"는 서명하지 않은 데이터에 포함된 텍스트 필드를 나타낸다. 〔The tokens specified in clauses 5 of this part of ISO/IEC 9798 contain text fields. The actual use of and the relationships between the various text fields in a given pass depend on the application. Some examples are given

below. If a signature scheme without message recovery is used and if the signed text field is not empty then the verifier needs to be in possession of the text prior to verifying the signature. In this annex "signed text fields" refers to text fields in the signed data and "unsigned text fields" refers to text fields in the unsigned data.]

예를 들어 메시지 복원이 없는 디지탈 서명이 사용되었다면, 데이터 출처 인증에 필요한 정보는 반드시 서명한 텍스트 필드와 토큰 속의 서명하지 않은 텍스트 필드의 일부분으로 포함되어 있어야 한다. [For example, if a digital signature scheme without message recovery is used, any information requiring data origin authentication should be placed in the signed text field and (as part of) the unsigned text field in the token.]

만약 토큰에 (충분한) 용장이 없다면, 암호화된 텍스트 필드를 사용하여 추가의 용장을 제공할 수 있다. [If the tokens do not contain (sufficient) redundancy, the enciphered text fields may be used to provide additional redundancy.]

텍스트 필드에는 추가의 시간변이 변수들을 포함될 수 있다. 예를 들어, 만약 텍스트 필드가 일련번호를 사용한다면, 5.1.1에서 사용된 Token AB의 텍스트 필드 안에 시각표를 포함할 수 있다. 이렇게 하면 인증 요청의 일부로 일련번호를 받아들일 때 사전에 시간 간격(time window)을 명시하지 않아도 "의도적인 지연"(forced delay)을 찾아낼 수 있다(부록 C 참조). [Text fields may contain additional time variant parameters. For instance a time stamp may be included in the text fields of TokenAB in mechanism 5.1.1 if this is used with sequence numbers. This would allow the detection of forced delays without having previously specified a time window for the acceptance of the sequence number as part of the authentication request (see also annex C).]

서명한 텍스트 필드는 토큰이 오직 실체인증을 위한 것임을 표시하는데 이용할 수 있다. 만약 한쪽 실체가 나쁜 의도를 가지고 잘못된 값을 선택해서 다른쪽 실체가 잘못된 서명을 하도록 하는 것을 방지하기 위해서, 다른 실체는 텍스트 필드에 난수값을 넣을 수도 있다. [Signed text fields may be used to indicate that the token is only valid for the purpose of entity authentication. Should there be a concern that one entity might choose a "degenerate" value with malicious intent for the other entity to sign, the other entity may introduce a random number in the text field.]

만약 특정한 주장자가 모든 검증자에게 똑같은 키를 사용한다는 사실에 근거해서 성공할 수 있는 어떤 공격 알고리듬이 있을 것으로 염려한다면, 서명한 텍스트 필드와 필요하다면 서명하지 않은 텍스트 필드에 원하는 검증자의 실체명을 포함시켜야 한다. [Should an algorithm be used where it may be possible to launch attacks based on the fact that a particular claimant communicates, and if such attacks are considered to be a threat, the identity of the intended verifier should be included in the signed text field and, if necessary, in the unsigned text field.]

주장자가 주장하고 있는 (인증되지 않은) 실체에 대한 정보를 검증자에게 알려주기 위해서 서명하지 않은 텍스트 필드를 사용할 수 있다. 만약 공개키의 분배를 위해서 인증서 외의 다른 수단을 이용한다면, 검증자에게 어떤 공개키가 주장자를 인증하기 위해서 사용되는지 알려주는 정보가 필요하다. [Unsigned text fields can also be used to provide information to a verifier indicating the (unauthenticated) identity which a claimant is claiming. If means other than certificates are used for distributing public keys, such information may be required to allow a verifier to determine which public key is to be used to authenticate a claimant.]

텍스트 필드는 또한 키를 분배하는데 사용할 수 있다(ISO/IEC 11770-3 참조). [Text fields could also be used for the distribution of keys (see ISO/IEC 11770-3).]

만일 ISO/IEC 9798의 제 3부에서 규정한 어떤 기법들을 어느 한쪽의 실체라도 인증을 시작할 수 있도록 하기 위해서 그 기법들을 시작하기 전에 추가적인 메시지를 사용하는 응용 분야에 이용하였다면, 침입자의 어떤 형태의 공격이 있을 수 있다. 텍스트 필드에 인증을 요구한 객체가 누구인가를 포함시킴으로써, 침입자가 불법적으로 획득한 토큰을 재사용하여 할 수 있는 공격을 막을 수 있다. [Should any of the mechanisms specified in this part of ISO/IEC 9798 be embedded in an application which allows either entity to initiate the authentication by using an additional message prior to the start of the mechanism, certain intruder attacks may become possible. Text fields may be used to state which entity requests the authentication in order to counteract such attacks, which are characterized by the fact that an intruder may reuse a token obtained illicitly.]

부록 B [Annex B]
(참고) (informative)
인증서 [Certificates]

ISO/IEC 9798의 제 3부에서 인증서는 공개키의 인증을 위해 사용할 수 있다. 이 경우에 인증서는 실체의 실체명과 공개키 그리고 가능한 다른 정보(예를 들어, 인증서의 유효기간이나 고유 번호)들을 포함한다. 인증서는 이런 데이터들과 함께 신뢰성 있는 제3자의 서명으로 구성되어 있다. [In this part of ISO/IEC 9798 certificates can be used to ensure the authenticity of public keys. In this case, a certificate contains an entity's distinguishing identifier, the entity's public key, and possibly other information (such as a validity period for the certificate and/or a serial number). The certificate consists of this collection of data, together with the signature of a trusted third party on this data.]

인증서의 검증은 신뢰성 있는 제3자의 서명 검증과, 필요하다면 폐지 시기나 유효기간 등의 인증서의 타당 조건의 확인으로 이루어진다. [The verification of a certificate consists of verifying the signature of the trusted third party, and checking, if required, other conditions related to the validity of the certificate such as the revocation or the validity period.]

인증서가 공개키 인증을 위한 유일한 방법은 아니다. 여러 가지 방법으로 다른 실체의 공개키를 얻을 수 있도록 하기 위해서, ISO/IEC 9798의

제3부에서 서술된 모든 인증 기법에서는 인증서의 사용을 선택 사항으로 했다. [Certificates are not the only way of guaranteeing the authenticity of public keys. To allow an entity to obtain the public keys of other entities by other means, the use of certificates is optional in all mechanisms in this part of ISO/IEC 9798.]

부록 C [Annex C]
(참고) (informative)
시간변이 변수들
[Time variant parameters]

시간변이 변수들은 고유성과 적시성을 관리하는데 사용한다. 이들은 이미 전송된 메시지들을 재사용하는 것을 찾아낼 수 있게 한다. 이러한 목적을 이루기 위하여, 어떤 메커니즘에 대해서 한 번 교환된 인증정보는 다음에 다시 교환할 때 변해야 한다. 검증자는 이 인증정보의 변화를 직접적으로 혹은 간접적으로 관리해야 한다. [Time variant parameters are used to control uniqueness / timeliness. They enable the replay of previously transmitted messages to be detected. To achieve this, the authentication information should vary from one use of the mechanism to the next. The verifier should have either mechanism to the next. The verifier should have either direct or indirect control over this variation.]

어떤 시간변이 변수들은 의도적인 지연(침입자가 통신 매체에 의도적으로 생기게 한 지연)을 찾아낼 수 있게 해준다. 두 번 이상의 전송이 필요한 인증기법에서는 다른 방법들 (즉, 특정 메시지들 사이의 최대 허용 시간 간격을 정하여 사용하는 "종료 시계"의 이용)을 사용하여 "의도적인 지연"을 찾아낼 수가 있다. [Some types of time variant parameters may also allow the detection of "forced delays"(delays introduced into the communication medium by an adversary). In mechanisms involving more than one pass, forced delays may also be detected by other means (such as "timeout clocks" used to enforce maximum allowable time gaps between specific messages).]

ISO/IEC 9798의 제3부에서 사용되는 시간변이 변수들의 세 가지 유형은 시각표, 일련번호 그리고 난수값이다. 구현 사양은 다른 응용 분야에 따라서 그 응용에 더 적합한 여러 유형의 시간변이 변수들이 필요하다. 어떤 경우에는 두 개 이상의 시간변이 변수들을 (예: 시각표와 일련번호) 사용하는게 더 적합하다. 시간변이 변수들의 선택에 관련한 세부적인 것은 본 ISO/IEC 9798의 제3부의 범위에서 벗어나므로 여기서는 논의하지 않는다. [The three types of time variant parameters used in this part of ISO/IEC 9798 are time stamps, sequence numbers and random numbers. Implementation requirements may make different time variant parameters preferable in different applications. In some cases, it may be appropriate to use more than one type of time variant parameters(e.g., both time stamps and sequence numbers). Details regarding the choice of these parameters are beyond the scope of this part of ISO/IEC 9798.]

C.1 시각표 [Time stamps]

시각표를 사용하는 인증기법은 통신을 하는 주장자와 검증자를 논리적으로 연결시켜 주는 공통

참조 시간을 사용한다. 권장하는 참조 시간은 Coordinated Universal Time(UTC)이다. 검증자는 고정된 크기의 허용 시간 간격을 설정하여 사용한다. 적시성은 검증되었고 수신된 토큰 안의 시각표와 그 토큰을 받은 시간과의 차를 검증자가 계산함으로써 관리된다. 만약 그 차가 설정한 시간 간격 안에 있다면 그 메시지를 받아들인다. 검증자는 현재의 시간 간격 안에 모든 메시지를 기록하고, 그 시간 간격 안에 기록된 메시지와 동일한 모든 메시지에 대해서는 거절함으로써 고유성을 검증할 수 있다. [Mechanisms involving time stamps make use of a common time reference which logically links two communicating parties. The recommended reference clock is Coordinated Universal Time (UTC). An acceptance window of some fixed size is used by the verifier computing the difference between the time stamp in a verified received token and the time as perceived by the verifier when the token is received. If the difference is within the window, the message is accepted. Uniqueness can be verified by logging all messages within the current window, and rejecting the second and subsequent occurrences of identical messages within that window.]

주장자와 검증자가 공유하는 시간 참조를 검증자가 (간접적으로) 관리할 수 있도록 하기 위해서는 시계의 동기화를 보증하는데 어떤 방법을 사용해야 한다. 또한 시계는 재사용에 의한 위장의 가능성 (어떤 객체가 다른 객체라고 거짓 주장하는 행위)을 줄이기 위해서 동기화가 잘되어야 한다. 특히 통신하는 두 객체가 참조하는 시계와 같은 시각표의 검증에 관련된 정보는 허가 없이 변경하거나 지움에 대해서 보호해야 한다. [Some mechanism should be used to ensure that the time clocks of the communicating parties are synchronised, in order that the time reference be under the verifier's (indirect) control. Moreover, time clocks need to be synchronized well enough to make the possibility of impersonation by replay acceptably small. It should also be ensured that all information relevant to the verification of time stamps, in particular the time clocks of the two communicating parties, are protected against tampering.]

시각표는 의도적인 지연을 찾아낼 수 있게 해준다. [Time stamps allow the detection of forced delays.]

C.2 일련번호 [Sequence numbers]

검증자가 메시지의 재사용을 찾을 수 있도록 해주는 일련번호를 사용함으로써 고유성은 관리될 수 있다. 주장자와 검증자는 사전에 특별한 방법으로 메시지들의 순서 번호를 정하는 정책 수립에 동의해야 한다. 그것에 대한 일반적인 정책은 특정 번호는 오직 한번만 (또는 규정된 시간 간격 안에 오직 한번만) 수용될 수 있도록 하는 것이다. 검증자는 메시지를 받아서 그 메시지안의 일련번호가 이미 약속된 정책에 따라 보내졌는지를 검사한다. 이런 방법으로 검증자는 (간접적으로) 일련번호를 관리할 수 있다. 만약 동반된 일련번호가 이미 동의된 정책에 따라서 보내지지 않았다면 그 메시지는 거부된다. [Uniqueness can be controlled using sequence numbers as they enable a verifier to detect the replay of messages. A claimant and verifier agree beforehand on a policy for numbering messages in a particular manner, the general idea being that a message with a particular manner, the general idea being

that a message with a particular number will be accepted only once (or only once within a specified time period). Messages received by a verifier are then checked to see that the number sent with the message is acceptable according to the agreed policy. In this way, the sequence number is under the verifiers (indirect) control. A message is rejected if the accompanying sequence number is not in accordance with the agreed policy.〕

일련번호의 사용에는 추가적인 부기가 필요하다. 주장자는 이미 사용된 일련번호 또는 앞으로 사용 가능한 일련번호에 대한 기록을 보존할 필요가 있다. 주장자는 그가 앞으로 통신하고자 하는 모든 잠재적인 검증자들에 대한 그런 기록들을 보존할 필요가 있다. 마찬가지로, 검증자도 모든 잠재적인 주장자들에 대한 기록들을 보존해야 한다. 시스템 다운과 같은 상황이 발생하여 정상적인 일련번호 작업을 유지할 수 없게 된다면, 일련번호 카운터를 재시동하거나 재설정하기 위한 특별한 절차가 필요하다. 〔Use of sequence numbers may require additional "book keeping". A claimant should maintain records of sequence numbers which have been used previously and/or sequence numbers which remain valid for future use. The claimant should keep such records for all potential verifiers with whom the claimant may wish to communicate. Similarly, the verifier should maintain such records corresponding to all potential claimants. Special procedures may also be required to reset and/or restart sequence number counters when situations (such as system failures) arise which disrupt normal sequencing.〕

검증자는 주장자가 사용하는 일련번호를 가지고서 의도적인 지연을 찾아낼 수 없다. 〔Use of sequence numbers by a claimant does not guarantee that a verifier will be able to detect forced delay.〕

C.3 난수값 〔Random numbers〕

ISO/IEC 9798의 제 3부에 규정된 인증기법들에 난수값들을 사용하면 재사용과 끼워넣기 공격을 막을 수 있다. 본 표준에서 사용되는 난수값은 예측할 수 없는 pseudo 난수값도 포함한다. 〔The random numbers used in mechanisms specified in this part of ISO/IEC 9798 prevent reply attacks or interleaving attacks. In the context of this part of ISO/IEC 9798 the use of the term random numbers also includes unpredictable pseudo-random numbers.〕

재사용이나 끼워넣기 공격을 막아내기 위해 검증자는 난수값을 생성하고 주장자에게 보내고, 주장자는 그가 보내는 암호화된 토큰 안에 난수값을 포함함으로써 응답을 한다(이를 시도-응답 방법이라고 한다). 이 절차는 특정 난수값을 포함하는 두 메시지들을 연결시켜준다. 만약 검증자가 같은 난수값을 다시 사용한다면, 제 3 자는 그 난수값이 있는 인증교환을 기록해 두었다가 검증자에게 이 기록된 토큰을 보냄으로써 검증자가 제 3자를 주장자라고 잘못 인증할 수 있다. 이러한 종류의 공격을 막기 위해 난수값은 재반복 되지 않을 확률이 매우 높아야 한다. 〔In other to prevent replay or interleaving attacks, the verifier obtains a random number which is sent to the claimant, and the claimant responds by including the random number in the enciphered part of the returned token(This is commonly referred to as challenge

response). This procedure links the two messages containing the particular random number. If the same random number is used by the verifier again, a third party that recorded the original authentication exchange can send the recorded token to the verifier and falsely authenticate itself as the claimant. In order to prevent such attacks, it is necessary for the random numbers to be non-repeating with a very high probability.〕

서명자는 다른 사람이 숨은 의도로 조작한 데이터에 자신이 서명하는 것을 방지하기 위하여, 서명하고자 하는 데이터에 그 자신의 난수값을 포함시킨다. 예측 불가능성으로 사전에 조작된 데이터에 서명하는 것을 방지한다. 〔The signing by one entity of a data block which has been manipulated by a second entity for some ulterior motive can be prevented by the first entity including its own random number in the data block which it signs. In this case, it is the unpredictability which prevents the signing of pre-defined data.〕

난수값은 정의에 의해서 예측 불가능하다. 만약 난수값들을 충분히 넓은 범위에서 값들을 취한다면 재반복될 확률은 아주 낮다. 〔Random numbers are by definition unpredictable, and can be considered non-repeating with a high degree of probability if they take values from a sufficiently large range.〕

주장자가 난수값을 사용한다고 해도 의도적인 지연을 찾아낼 수는 없다. 〔Use of random numbers by a claimant does not guarantee that a verifier will be able to detect forced delays.〕

부록 D 〔Annex〕
참고 〔informative〕
Bibliography

〔1〕 ISO/IEC 9796: 1991, *Information technology - Security techniques - Digital signature scheme giving message recovery.*

〔2〕 ISO/IEC 11770-3: 199?, *Information technology - Security techniques - Key Key management - Part 3: Mecha-nisms using asymmetric techniques.* (to be published)

(본 원고를 정리하는 데에 수고를 해 준 대학원생 이 준호, 문 순일, 최 송관에게 감사를 표한다.)

□ 著者紹介

이 필 중 (李 弼 中) 종신회원

1951년 12월 30일생
1974년 2월 서울대학교 전자공학과 학사
1977년 2월 서울대학교 전자공학과 석사
1982년 6월 U.C.L.A. System Science, Engineer
1985년 6월 U.C.L.A. Electrical Engineering, Ph.D.
1980년 6월 ~ 1985년 8월 Jet Propulsion Laboratory, Senior Engineer
1985년 8월 ~ 1990년 2월 Bell Communications Research, M.T.S.
1990년 2월 ~ 현재 포항공과대학 전자전기공학과, 부교수