通信情報保護學會誌
第5卷 第3號, 1995. 9

ISO/IEC JTC1/SC27의 국제표준소개 (9) : ISO/IEC IS9798-4 정보기술 - 보안기술 - 실체인증 기법, 제 4 부: 암호학적 확인 함수를 이용한 인증

(Information technology - Security techniques - Entity authentication, Part 4 : Mechanisms using a cryptographic check function)

이 필 중*

요 약

제 5권 제 1호에 이어 상대방이 자신이라고 주장한 실체가 정말 그 실체인지를 인증하기 위한 기법을 표준화하는 과제 중의 네번째로 "암호학적 확인 함수를 이용한 인증"을 소개한다. 이 과제는 제 2부인 "대칭형 암호기술을 이용한 인증"과 많이 유사하므로 쉽게 진행되어 1993년에 CD(Committee Draft), 1994년 DIS(Draft for International Standard)가 되었고 1995년에 IS(International Standard)가 되었으며 1999년에 1차 검토가 있을 예정이다.

1. 범 위 [Scope]

ISO/IEC 9798의 제4부에서는 암호학적 확인 함수를 사용하는 4개의 실체 인증기법을 규정하고 있다. 그 중 두 개는 단일 실체(일방) 인증기법이고, 다른 두 개는 두 실체간의 상호 인증기법이다. [This part of ISO/IEC 9798 specifies entity authentication mechanism using a cryptographic check function. Two mechanisms are concerned with the authentication of a single entity (unilateral authentication), while the remaining are mechanisms for mutual authentication of two entities.]

ISO/IEC 9798의 제4부에서 설명되는 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

* 종신회원, 포항공과대학교 전자전기공학과

information from being accepted at a later time.]

시각표나 일련번호를 사용하면 1회 전송으로 일방인증을 할 수 있고, 상호인증을 위해서는 2회 전송이 필요하다. 난수값을 사용하는 도전-응답 방법일때는 일방인증을 위해서 2회 전송이 필요하며, 상호인증을 위해서는 3회 전송이 필요하다. [If a time stamp or 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 passes are required to achieve mutual authentication.]

암호학적 확인 함수의 예는 부기 C에 있다. [Examples of cryptographic check functions are given in annex C.]

2. 참고 문헌 [Normative reference]

아래의 표준 ISO/IEC 9798의 제1부-일반 모델은 본문의 참고 문헌으로서 ISO/IEC 9798의 제4부에서 필요한 내용들을 포함하고 있다. 아래의 표준은 본 표준이 발표될 당시에는 유효했다. 모든 표준들은 개정되기 마련이므로, ISO/IEC 9798의 제4부를 근거로 삼으려는 사람들은 아래에 명시한 표준의 최신 개정본을 찾아보기 바란다. ISO와 IEC는 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 9798의 제4부에서 사용될 정의와 표기법들은 ISO/IEC 9798-1에서 기술된 것을 적용한다. 추가로 다음의 정의와 표기가 사용된다. [For the purposes of this part of ISO/IEC 9798 the definitions and notation described in ISO/IEC 9798-1 apply. In addition the following definition and notation are used:]

암호학적 확인 값: 데이터 유니트에 암호학적 변환을 적용하여 얻은 정보[ISO 7498-2]

$f_K(Z)$: 비밀키 K와 임의의 데이터 스트링 Z를 암호학적 확인 함수 f의 입력으로 하여 얻은 결과인 암호학적 확인 값

$\begin{matrix} T_A \\ N_A \end{matrix}$: 실체 A가 생성한 시간 변이 변수로 시각표 T_A나 일련번호 N_A [cryptographic check value : Information which is derived by performing a cryptographic transformation on the data unit [ISO 7498-2]. $f_K(Z)$: Cryptographic check value which is the result of applying the cryptographic check function f using as input a secret key K and an arbitary data string Z. $\begin{matrix} T_A \\ N_A \end{matrix}$:Time variant parameter originated

by entity A which is either a time stamp T_A or a sequence number N_A.]

4. 요구조건 [Requirements]

ISO/IEC 9798의 제4부에서 기술하는 인증기법은 인증되어야 할 실체가 비밀 인증키를 알고 있음을 보여줌으로써 자신의 실체를 증명하는 것이다. 인증되어야 할 실체는 비밀키로 특정한 데이타를 암호학적 확인 함수에 적용시켜 암호학적 확인 값을 얻는다. 이 암호학적 확인 값은 실체의 비밀키를 알고 있고 암호학적 확인 값을 다시 계산하여 받은 값과 비교해 볼 수 있는 어느 누구에 의해서도 확인될 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 a secret authentication key. This is achieved by the entity using its secret key with a cryptographic check function applied to specific data to obtain a cryptographic check value. The cryptographic check value can be checked by anyone knowing the entity's secret authentication key who can re-calculate the cryptographic check value and compare it with the value received.]

인증기법들은 다음의 요구조건들이 있다. 이들 중에 하나라도 충족되지 않으면 인증절차는 위태롭게되거나 구현될 수 없다. [The authentication mechanisms have the following requirements. If any one of these is not met then the authentication process may be compromised or it cannot be implemented.]

a) 검증자에게 자신을 인증하려는 주장자는 검증자와 공통의 비밀 인증키를 공유할 수 있다. 이 키는 특정한 인증기법이 수행되기 전에 인증에 참여하는 각 실체에게 알려져야 한다. 이 국제표준에서는 이 과정에 대해 구체적으로 다루지 않는다. [a) A claimant authenticating itself to a verifier shares a common secret authentication key with that verifier. This key shall be known to the involved entities prior to the commenc-ement of any particular run of an authentication mechanism. The method by which the key is distributed to the entities is beyond the scope of this part of ISO/IEC 9798.]

b) 주장자와 검증자에 의해 공유된 비밀 인증키는 오직 그 두 측에게만 알려지거나 그들 모두가 신뢰하고 있는 제3의 실체에게도 알려질 수 있다. [b) The secret authentication key, shared by a claimant and a verifier, shall be known only to those two entities and, possibly to other parties they both trust.]

c) 비밀 키 K와 임의의 데이터 스트링 Z를 입력으로 하여 $f_K(Z)$를 만드는 암호학적 확인 함수 f는 다음의 성질을 만족한다: [c) The cryptographic check function f which takes as input a secret key K and an arbitrary string Z to produce $f_K(Z)$ shall satisfy the following properties:]

- 어떤 키 K와 데이터 스트링 Z에 대해서도 $f_K(Z)$를 계산하는 것이 가능해야 한다.
- $Y_j(j = 1, 2, \ldots, i\text{-}1)$를 관찰한 후에 선택될 수 있는 X_i에 대하여 $f_K(X_i) = Y_i(i = 1, 2, \ldots)$를 만족하는 (X_i, Y_i)에 대한 정보를 알더라도, 사전 정보가 주어지지 않은 어떤 고정된 키 K에 대해서도 $f_K(X) = Y$를 만족하는 새로운 (X, Y)를 찾는 것이 계산상 불가능해야 한

다. [- for any key K and data string Z it shall be practical to compute $f_K(Z)$; - for any fixed key K, and given no prior knowledge of K, it shall be computat-icnally infeasible to find a new pair (X, Y) such that $f_K(X) = Y$, even given knowledge of a set of pairs (X_i, Y_i) such that $f_K(X_i) = Y_i (i = 1, 2, \ldots,$ where the value of X_i may have been chosen after observing the value of Y_j $(j = 1, 2, \ldots, i-1)$.]

d) 인증기법의 안전도는 키의 길이와 비밀성, 암호학적 확인 함수의 성질, 그리고 확인값의 길이에 영향을 받는다. 이 변수들은 요구되는 보안 등급을 맞추기 위해 선택될 수 있고 보안 정책에 따라 명시될 수도 있다. [d) The strength of the mechanisms is dependent on the length and the secrecy of the key, on the nature of the cryptographic check function, and on the length of the check value. These parameters shall be chosen to meet the required security level, as may be specified by the security policy.]

5. 인증기법 [Mechanisms]

이들의 인증기법에서 두 실체 A, B는 특정한 인증기법이 수행되기 전에 공통 비밀 인증키 K_{AB} 나 두 개의 한 방향 비밀키인 K_{AB}, K_{BA}를 공유한다. 후자의 경우에 한 방향 키 K_{AB}와 K_{BA}는 각각 B에 의한 A의 인증과 A에 의한 B의 인증에 사용된다. [In these authentication mechanisms the entities A and B shall share a common secret authentication key K_{AB} or two uni-directional secret keys K_{AB} and K_{BA} prior to the commencement of any particular run of the authentication mechanisms. In the latter case the unidirectional keys K_{AB} and K_{BA} are used respectively for the authentication of A by B and of B by A.]

그 기법들은 시각표, 일련번호 또는 난수값 등의 시간변이 변수들의 사용이 필요하다. 특히 인증키의 유효시간내에 반복되지 않는 이들 변수들은 인증기법의 안전성을 위해 매우 중요하다. 좀 더 자세한 내용은 부기 B를 참조하라. [The mechanisms require the use of time variant parameters such as time stamps, sequence numbers or random numbers. The properties of these parameters, in particular that it is most unlikely for them to repeat within the life-time of an authentication key, are important for the security of these mechanisms. For additional information see annex B.]

다음의 기법에서 명시된 텍스트 필드들은 ISO/IEC 9798의 제4부의 범위 밖의 응용에 유용하게 쓰일 수 있다(그들은 공란일 수도 있다). 그들의 관계와 내용은 특정한 응용에 달려있다. 텍스트 필드의 사용에 대한 자세한 내용은 부기 A를 참조하라. [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 relation and contents further depend upon the specific application. See annex A for information on the use of text field.]

검증자가 텍스트 필드를 독립적으로 알 수 있을 때만 -예를 들어 미리 알려져 있거나 암호화하지 않고 보내지거나 유추될 수 있다면- 텍스트 필드는 암호학적 확인 함수의 입력으로 포함될 수 있다. [A text field may only be included in the input to the cryptographic check function if the verifier can determine it

independently, e. g., if it is known in advance, sent in clear or can be derived from one or both of those sources.]

5.1 일방인증 [Unilateral authentication]

일방인증이란 두 실체중 단지 한 실체만이 인증기법에 의해 인증 받는 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 인증기법에서 주장자 A가 인증을 시작하고, 검증자 B에 의해 인증을 받는다. 유일성과 적시성은 시각표 또는 일련번호를 발생시키고 확인함으로써 관리된다(부기 B 참조). [In this authentication mechanisms 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 B).]

이 인증기법은 그림 1에 나타나 있다. [The authentication mechanisms is illustrated in figure 1.]

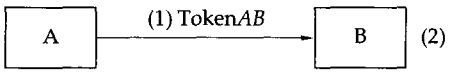

그림 1

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

$$\text{Token}AB = {}^{T_A}_{N_A}\,||\text{Text2}||\, f_{K_{AB}}({}^{T_A}_{N_A}\,||\text{B}||\text{Text1}),$$

여기서 주장자 A는 시간변이 변수로 일련번호 N_A나 시각표 T_A를 사용한다. 시간변이 변수의 선택은 두 실체의 기술적인 역량과 환경에 달려있다. [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.]

TokenAB에서 실체명 B를 포함하는 것은 선택적이다. [The inclusion of the distinguishing identifier B in TokenAB is optional.]

주 TokenAB에 실체명 B를 포함시킴으로서, 악의를 갖는 침입자가 마치 자기가 B인 것처럼 가장하여 실체 A에게 TokenAB를 재사용하는 것을 막을 수 있다. 그러한 공격이 발생하지 않는 환경에서는 생략될 수도 있어서 식별자 B를 포함하는 것은 선택사항이 되었다. 그리고 한 방향 키가 사용된다면 실체명 B는 생략될 수도 있다. [NOTE - Distinguishing identifier B is included in TokenAB to prevent the reuse of TokenAB on entity A by an adversary masquerading as entity B. Its inclusion is made optional so that, in environments where such attacks cannot occur, it may be omitted. The distinguishing identifier B may also be omitted if a uni-directional key is used.]

(1) A가 B에게 TokenAB를 보낸다.
(2) B는 TokenAB를 포함하고 있는 메세지

를 받아 시각표나 일련번호를 확인하고 $f_{K_{AB}}(\begin{smallmatrix}T_A\\N_A\end{smallmatrix} \| B \| \text{Text1})$를 계산하여 토큰 안의 암호학적 확인 값(만약 있다면)과 비교하여 N_A 실체명 B와 시각표나 일련번호의 옳음을 검증하여 토큰을 검증한다. [(1) A sends TokenAB to B. (2) On receipt of the message containing TokenAB, B verifies TokenAB by checking the time stamp or the sequence number, calculat-ing $f_{K_{AB}}(\begin{smallmatrix}T_A\\N_A\end{smallmatrix} \| B \| \text{Text1})$ and comparing it with the cryptographic check value of the token, thereby verifying the correctness of the distinguishing identifier B, if present, as well as the time stamp or the sequence number.]

5.1.2 2회 전송 인증
[Two pass authentication]

이 인증기법에서 주장자 A는 인증과정을 시작하는 검증자 B에 의해서 인증을 받게 된다. 유일성과 적시성은 난수값 R_B를 발생시키고 확인함으로써 관리된다(부기 B 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 R_B (see annex B).]

이 인증기법은 그림 2에 나타나 있다. [The authentication mechanisms is illustrated in figure 2.]

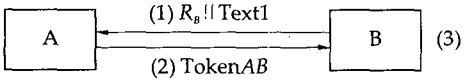

그림 2

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

TokenAB = Text3 || $f_{K_{AB}}(R_B \| B \| \text{Text2})$

TokenAB에서 실체명 B를 포함하는 것은 선택적이다. [The inclusion of the distinguishing identifier B in TokenAB is optional.]

주 TokenAB에 실체명 B가 들어있는 것은 소위 반사공격이라는 것을 막기 위해서이다. 그러한 공격은 침입자가 A인척하고 난수값 R_B를 B에게 "반사"하는 것을 의미한다. 그러한 공격이 발생하지 않는 곳에서는 생략될 수도 있어서 실체명 B를 포함하는 것은 선택사항이 되었다. 그리고 한 방향 키가 사용된다면 실체명 B는 생략될 수도 있다. [NOTE - Distinguishing identifier B is included in TokenAB to prevent a so - called reflection attack. Such an attack is characterized by the fact that an intruder "reflects" the challenge R_B to B pretending to be A. The inclusion of the distinguishing identifier B is made optional so that, in environments where such attacks cannot occur, it may be omitted. The distinguishing identifier B may also be omitted if a uni-directional key is used.]

(1) B가 A에게 난수값 R_B와 선택적으로 텍스트 필드 Text1을 보낸다.
(2) A가 B에게 TokenAB를 보낸다.
(3) B는 TokenAB를 포함하고 있는 메세지를 받아 $f_{K_{AB}}(R_B \| B \| \text{Text2})$를 계산하여 토큰의 암호학적 확인 값(만약 있다면)과 비교하여 실체명 B와 단계 (1)에서 A에게 보낸 난수값 R_B가 TokenAB

에 있는 난수값과 같은지를 검사함으로써 TokenAB를 검증한다. [(1) B sends a random number R_B and, optionally, a text field Text1 to A. (2) A sends TokenAB to B. (3) On receipt of the message containing TokenAB, B verifies TokenAB by calculating $fk_{AB}(R_B \,||B||$ Text2) and comparing it with the cryptographic check value of the token, thereby verifying the correctness of the distinguishing identifier B, if present, and that the random number R_B, sent to A in step (1), was used in constructing TokenAB.]

5.2 상호인증 [Mutual authentication]

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

상호인증을 하기 위해서 5.1.1과 5.1.2절에서 설명된 두 기법이 각각 5.2.1과 5.2.2절에서 채택된다. 각각의 경우에서 1회의 전송이 추가되므로 2번의 단계가 더 필요하게 된다. [The two mechanisms described in 5.1.1 and 5.1.2 are adapted in 5.2.1 and 5.2.2, respectively, to achieve mutual authentication. In both cases this requires one more pass resulting in two more steps.]

주 상호인증의 세 번째 기법은 5.1.2에 명시된 두 가지의 경우로부터 만들어질 수 있는데 하나는 A에 의해서 시작되고 나머지 하나는 B에 의해서 시작된다. [NOTE - A third mechanism for mutual authentication can be constructed from two instances of the mechanism specified in 5.1.2, one started by entity A and the other by entity A.]

5.2.1 2회 전송 인증 [Two pass authentication]

이 상호인증기법에서 유일성과 적시성은 시각표나 일련번호를 발생시키고 확인함으로써 관리된다(부기 B 참조). [In this authentication mechanism uniqueness/timeliness is controlled by generating and checking time stamps or sequence numbers (see annex B).]

이 인증기법은 그림 3에 나타나 있다. [The authentication mechanism is illustrated in figure 3.]

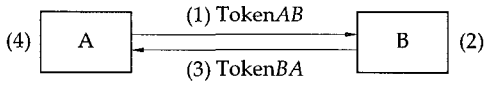

그림 3

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

$$\text{Token}AB = {}^{T_A}_{N_A}||\text{Text2}||\, fk_{AB}({}^{T_A}_{N_A}||B||\ \text{Text1}).$$

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

$$\text{Token}BA = {}^{T_B}_{N_B}||\text{Text4}||\, fk_{AB}({}^{T_B}_{N_B}||A||\ \text{Text3}).$$

TokenAB에 실체명 B를 포함하는 것과 TokenBA에 실체명 A를 포함하는 것은 (독립

적으로) 선택적이다. [The inclusion of the distinguishing identifier *B* in Token*AB* and the inclusion of the distinguishing identifier *A* in Token*BA* are (independently) optional.]

주1 Token*AB*에 실체명 *B*를 포함시킴으로서, 악의를 갖는 침입자가 마치 자기가 B인 것처럼 가장하여 실체 *A*에게 Token*AB*를 재사용하는 것을 막을 수 있다. 같은 이유로 실체명 *A*가 Token*BA*에 포함되었다. 그러한 공격이 발생하지 않는 환경에서는 생략될 수도 있어서 실체명을 포함하는 것은 선택사항이 되었다. 그리고 한 방향 키(아래를 보라)가 사용된다면 실체명 *A*와 *B*는 생략될 수도 있다. [NOTE1 - Distinguishing identifier *B* is included in Token*AB* to prevent the re-use of Token*AB* on entity *A* by an adversary masquerading as entity *B*. For similar reasons the distinguishing identifier *A* is present in Token*BA*. Their inclusion is made optional so that, in environments where such attacks cannot occur, one or both may be omitted. The distinguishing identifiers *A* and *B* may also be omitted if uni-directional keys (see below) are used.]

시각표를 사용하는 것과 일련번호를 사용하는 것중의 하나를 선택하는 것은 주장자와 검증자의 기술적인 역량과 환경에 달려있다. [The choice of using either time stamps or sequence numbers in this mechanism depends on the capabilities of the claimant and the verifier as well as on the environment.]

단계 (1), (2)는 5.1.1의 1회 전송 인증에서와 같다.

(3) *B*가 *A*에게 Token*BA*를 보낸다.

(4) 단계 (3)에서 보내진 메세지는 5.1.1절의 단계 (2)와 같은 방법으로 처리된다. [Steps (1) and (2) are identical to those specified in 5.1.1, one pass authentication. (3) *B* sends Token*BA* to *B*. (4) The message in step (3) is handled in a manner analogous step (2) of 5.1.1.]

주2 이 기법에서 두 개의 메세지는 단시 적시성에 의해서 막연히 결합되어 있을뿐이다; 그 기법은 5.1.1의 기법을 독립적으로 두번 사용한다. 이 두 메세지를 좀 더 강하게 묶으려면 텍스트 필드를 적절히 사용해야 한다 (부기 A 참조). [NOTE 2 - The two message 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. Further binding together of these messages can be achieved by making appropriate use of the text fields (see annex A).]

한 방향 키가 사용된다면 Token*BA*와 단계 (4)에서 쓰여지던 키 K_{AB}는 한 방향 키 K_{BA}로 대치된다. [If uni-directional keys are used then the key K_{AB} in Token*BA* is replaced by the uni-directional key K_{BA} and the appropriate key is used in step(4)]

5.2.2 3회 전송 인증
[The Three pass authentication]

이 상호인증기법에서 유일성과 적시성은 난수값을 발생시키고 확인함으로써 관리된다 (부기 B 참조). [In this mutual authentication mechanism uniqueness/timeliness is controlled by generating and checking random numbers (see annex B).]

이 인증기법은 그림 4에 나타나 있다. [The authentication mechanism is illustrated in figure 4.]

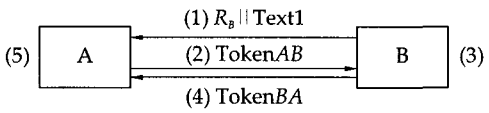

그림 4

토큰의 형식은 다음과 같다. [The tokens are of the following form:]

$$\text{Token}AB = R_A \,||\, \text{Text3} \,||\, f_{K_{AB}}(R_A \,||\, R_B \,||\, B \,||\, \text{Text2}),$$

$$\text{Token}BA = \text{Text5} \,||\, f_{K_{AB}}(R_B \,||\, R_A \,||\, \text{Text4}).$$

주1 TokenBA에 R_B를 포함시키는 것은 TokenAB에서 TokenBA를 유도하는 것을 막기 위한 것이다. [NOTE 1 - The inclusion of R_B in TokenBA prevents the derivation of TokenBA from TokenAB.]

TokenAB에 실체명 B를 포함하는 것은 선택적이다. [The inclusion of the distinguishing identifier B in TokenAB is optional.]

주2 TokenAB에 실체명 B가 들어있는 것은 소위 반사공격이라는 것을 막기 위해서이다. 그러한 공격은 침입자가 A인척하고 난수값 R_B를 B에게 "반사"하는 것을 의미한다. 그러한 공격이 발생하지 않는 곳에서는 생략될 수도 있어서 실체명 B를 포함하는 것은 선택사항이 되었다. 그리고 한 방향 키(아래를 보라)가 사용된다면 실체명 B는 생략될 수도 있다. [NOTE 2 - Distinguishing identifier B is included in TokenAB to prevent a so-called reflection attack. Such an attack is characterized by the fact that an intruder "reflects" the challenge R_B to B pretending to be A. The inclusion of the distinguishing identifier B is made optional so that, in environments where such attacks cannot occur, it may be omitted. The distinguishing identifier B may also be omitted if uni-directional keys (see below) are used.]

(1) B가 A에게 난수값 R_B와 선택적으로 텍스트 필드 Text1을 보낸다.

(2) A가 B에게 TokenAB를 보낸다.

(3) B는 TokenBA를 포함하고 있는 메세지를 받아 $f_{K_{AB}}(R_A \,||\, R_B \,||\, B \,||\, \text{Text2})$를 계산하여 암호학적 확인 값과 비교하여 실체명 B(만약 있다면)와 단계 (1)에서 A에게 보낸 난수값 R_B가 TokenAB에 있는 난수값과 같은지를 확인함으로써 TokenAB를 검증한다.

(4) B가 A에게 TokenBA를 보낸다.

(5) A는 TokenBA를 포함하고 있는 메세지를 받아 $f_{K_{AB}}(R_B \,||\, R_A \,||\, \text{Text4})$를 계산하여 암호학적 확인 값과 비교하여 단계 (1)에서 B로 부터 받은 난수값 R_B와 TokenBA에 있는 난수 값과 같은지, 그리고 단계 (2)에서 B에게 보낸 난수값 R_A가 TokenBA에 있는 난수값과 같은지를 확인함으로써 TokenBA를 검증한다. [(1) B sends a random number R_B and, optionally, a text field Text1 to A. (2) A sends TokenAB to B. (3) On receipt of the message containing TokenAB, B verifies TokenAB by calculating $f_{K_{AB}}(R_A \,|\, R_B \,||\, B \,||\, \text{Text2})$ and comparing it with the cryptographic check value of the token, thereby verifying the correctness of the distinguishing identifier B, if present, and that the random number R_B, sent to A in step (1), was used in constr-

ucting Token*AB*. (4) *B* sends Token*BA* to *A*. (5) On receipt of the message containing Token*BA*, *A* verifies Token*BA* by calculating $f_{K_{AB}}(R_B \| R_A \|$ Text4) and comparing it with the cryptographic check value of the token, thereby verifying that the random number RB, received from *B* in step (1) was used in constructing in Token*BA* and that the random number R_A, sent to *B* in step (2), was used in constructing Token*BA*.]

한 방향 키가 사용된다면 Token*BA*와 단계 (5)에서 쓰여지던 키 K_{AB}는 한 방향 키 K_{BA}로 대치된다. [If uni-directional keys are used then the key K_{AB} in Token*BA* is replaced by the uni-directional key K_{BA} and the appropriate key is used in step (5).]

부기 A [Annex A]
(참고) (informative)
텍스트 필드의 사용
[Use of text fields]

ISO/IEC 9798의 제4부의 5절에서 규정된 토큰들은 텍스트 필드를 포함한다. 토큰의 전송에서 다양한 텍스트 필드들의 관계들과 실제적인 사용은 그 응용에 달려 있다. 예들을 살펴보면 다음과 같다. [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.]

기밀성과 데이타출처인증을 필요로 하는 모든 정보는 토큰내의 암호학적 확인 값의 계산에 이용되어야 한다. [Any information requiring data origin authentication should be used in the calculation of the cryptographic check value of the token.]

텍스트 필드는 추가의 시간변이 변수들을 포함할 수 있다. 예를 들어, 5.1.1절의 기법에서 일련번호가 사용된다면, Token*AB*의 텍스트 필드안에 시각표가 포함될 수 있다. 이 방법으로 메세지를 받은 수신자는 메세지에 포함된 시각표가 정해진 시간간격내(time window)에 있는가를 확인하게 함으로써 "강요된 지연" (forced delay)들을 찾아낼 수 있다(부기 B 참조). [Text fields may contain additional time variant parameters. For instance, if mechanism 5.1.1. is used with sequence numbers, then a time stamp may be included in the text fields of Token*AB*. This would allow the detection of forced delays by requiring the recipient of a message to verify that any time stamp contained in the message is within a prespecified time window (see also annex B).]

만약 두 개 이상의 적법한 키가 존재한다면, 평문 텍스트 필드는 키 식별자를 포함할 수 있다. [If more than one valid key exists, then the cleartext text field may include the key identifier.]

만약 ISO/IEC 9798의 제4부에서 규정된 어떤 기법들을 어느 한쪽의 실체라도 인증을 시작할 수 있도록 하기 위해서 그 기법들을 시작하기 전에 추가적인 메세지를 사용하는 응용분야에 이용한다면 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.]

부기 B [Annex B]
(참고) (informative)
시간변이 변수들
[Time variant parameters]

시간변이 변수들은 유일성과 적시성을 관리하는데 사용한다. 이들은 이미 전송된 메세지들을 재사용하는 것을 찾아낼 수 있게 한다. 이러한 목적을 이루기 위하여, 어떤 메카니즘에 대해서 한번 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 replay of previously transmitted messages to be detected. To achieve this, the authentication information should vary from one exchange instance to the next. The verifier should have either direct or indirect control over this variation.]

어떤 시간변이 변수들은 강요된 지연(침입자가 통신매체에 의도적으로 생기게 한 지연)을 찾아낼 수 있게 해준다. 두 번 이상의 전송이 필요한 인증기법에서는 다른 방법들(즉, 특정 메세지들 사이의 최대허용시간 간격을 정하여 사용하는 "종료 시계"의 이용)을 사용하여 강요된 지연을 찾아낼 수가 있다. [Some types of time variant parameters may also allow for 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 제4부에서 사용되는 시간변이 변수들의 세 가지 유형은 시각표, 일련번호 그리고 난수값이다. 구현 사양은 다른 응용분야에 따라서 그 응용에 더 적합한 여러 유형의 시간변이 변수들을 필요로 한다. 어떤 경우에는 두개 이상의 시간변이 변수들을 (예: 시각표와 일련번호) 사용하는 게 더 적합하다. 시간변이 변수들의 선택에 관련한 세부적인 것은 본 ISO/IEC 9798의 제4부의 범위에서 벗어남으로 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.]

B.1 시각표 [Time stamps]

시각표를 사용하는 인증기법은 통신을 하는 주장자와 검증자를 논리적으로 연결시켜 주는

공통참조시간을 사용한다. 권장하는 참조시간은 Coordinated Universal Time(UTC)이다. 검증자는 고정된 크기의 허용시간간격을 설정하여 사용한다. 적시성은 검증되었고 수신된 토큰안의 시각표와 그 토큰을 받은 시간과의 차를 검증자가 계산함으로써 관리된다. 만약 그 차가 설정한 시간간격안에 있다면 그 메세지를 받아들인다. 검증자는 현재의 시간간격안에 모든 메세지를 기록하고, 그 시간간격안에 기록된 메세지와 동일한 모든 메세지에 대해서는 거절함으로써 고유성을 검증할 수 있다. [Mechanisms involving time stamps make use of a common time reference which logically links a claimant and a verifier. The recommended reference clock is Coordinated Universal Time (UTC). An acceptance window of some fixed size is used by the verifier. Timeliness is controlled by the verifier computing the difference between the time stamp in a verified received token and the time as perceived by the verifier at the time 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 의해서 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 허가없이 변경하거나 지움에 대해서 보호되어야 한다. [Some mechanism should be used to ensure that the time clocks of the claimant and verifier 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 강요된 지연을 찾아낼 수 있게 해준다. [Mechanisms using time stamps allow the detection of forced delays.]

B.2 일련번호 [Sequence numbers]

검증자가 메세지의 재사용을 찾을 수 있도록 해주는 일련번호를 사용함으로써 유일성은 관리될 수 있다. 주장자와 검증자는 사전에 특별한 방법으로 메세지들의 순서 번호를 정하는 정책수립에 동의해야 한다. 그것에 대한 일반적인 정책은 특정 번호는 오직 한번만 (또는 규정된 시간간격안에 오직 한번만) 수용될 수 있도록 하는 것이다. 검증자는 메세지를 받아서 그 메세지안의 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 메세지는 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 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 along with the message is acceptable according to the agreed policy. In this way, the sequence number is under the verifier's (indirect) control. A message is rejected if the accompanying sequence number is not in accordance with the agreed policy.]

일련번호의 사용은 추가적인 부기가 필요하다. 주장자는 이미 사용된 일련번호 또는 앞으로 사용가능한 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 that 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 강요된 지연을 찾아낼 수 없다. 만약 메세지 송신자가 전송된 메세지의 시간과 돌려받은 어떤 응답 사이의 시간차를 측정하면, 두 개 또는 그 이상의 메세지를 사용하는 인증기법에 대해서는 강요된 지연을 찾아낼 수 있다. 그리고 만약 그 시간차가 정해진 허용시간 밖에 존재하면 그 메세지를 거부한다. [Use of sequence numbers by a claimant does not guarantee that a verifier will be able to detect forced delay. For mechanisms involving two or more messages, forced delays can be detected if the sender of a message measures the time interval between transmission of a message and receipt of an expected reply, and rejects it if the delay is more than a prespecified time slot.]

B.3 난수값 [Random numbers]

ISO/IEC 9798의 제4부에 규정된 인증기법들에 난수값들을 사용하면 재사용과 끼어넣기 공격을 막을 수 있다. 본 표준에서 사용되는 난수값은 예측할 수 없는 pseudo 난수값도 포함한다. [The random numbers as used in mechanisms specified in this part of ISO/IEC 9798 prevent reply 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 끼어넣기 공격을 막아내기 위해 검증자는 난수값을 생성하고 주장자에게 보내고, 주장자는 그가 보내는 암호화된 토큰안에 난수값을 포함함으로써 응답을 한다(이를 도전-응답 방법이라고 한다). 이 절차는 특정 난

수값을 포함하는 두 메세지들을 연결시켜 준다. 만약 같은 난수값이 검증자에 의해서 다시 사용되어진다면, 제3자는 그 난수값이 포함된 인증교환을 기록해두었다가 검증자에게 기록된 토큰을 보냄으로써 검증자가 제3자를 그가 주장하는 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 authentication data of 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.]

난수값은 정의에 의하서 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 강요된 지연을 찾아낼 수는 없다. [Use of random numbers by a claimant does not guarantee that a verfier will be able to detect forced delays.]

부기 C [Annex C]
참고 (informative)
암호학적 확인 함수의 예
[Examples of cryptographic check functions]

C.1 메세지 인증 알고리듬의 응용 [Application of message authentication algorithm]

암호학적 확인 값은 ISO/IEC 9798이나 ISO 8731-2에 명시된 것처럼 암호학적 확인 함수를 적용한 결과이다. [The cryptographic check value is the result of applying a cryptographic check function such as specified in ISO/IEC 9798 or ISO 8731-2.]

C.2 해쉬 함수와 관련된 암호화 알고리듬의 응용 [Application of encipherment algorithm combined with hash-function]

암호학적 확인 값은 ISO/IEC 10118에 명시된 해쉬 함수를 데이터 스트링 Z에 적용시켜 얻은 해쉬 코드에 비밀키 K를 사용하는 암호화 알고리듬을 적용한 결과이다. [The cryptographic check value is the result of applying an encipherment algorithm using the secret key K on the hash-code, obtained by applying a hash-function specified in ISO/IEC 10118 on the data string Z.]

부기 D [Annex D]
참고 (informative)
Bibliography

References

[1] ISO 7498-2 : 1089, Information processing systems - Open systems Interconnection - Basic Reference Mode - Part 2: Security Architecture.

[2] ISO 8731-1 : 1987, Banking - Approved algorithms for message authentication - Part 1 : DEA.

[3] ISO 8731-2 : 1992, Banking - Approved algorithms for message authentication - Part 2 : Message authenticator algorithm.

[4] ISO/IEC 9797 : 1994, Information technology - Security techniques - Data integrity mechanism using a crypto-graphic check function employing a block cipher algorithm.

[5] ISO 9807 : 1991, Banking and related financial services - Requirements for message authentication (retail).

[6] ISO/IEC 10118-1 : 1994, Information technology - Security techniques - Hash - functions - Part 1 : General.

[7] ISO/IEC 10118-2 : 1994, Information technology - Security techniques - Hash - functions - Part 2 : Hash - functions using an n - bit block cipher algorithm.

[8] ANSI X9.9 : 1986, Financial Institution Message Authentication (Wholesale).

[9] ANSI X9.19 : 1986, Financial Institution Retail Message Authentication.

(본 원고를 정리하는 데에 수고를 해 준 대학원생 정 경임에게 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