通信情報保護學會誌
第6卷 第3號, 1996. 9

ISO/IEC JTC1 SC27/WG2의 용어들에 관한 조사 연구

진 원 일*, 김 동 한*, 이 인 수*, 김 철**

요 약

본 고에서는 ISO/IEC JTC1 SC27/WG2의 용어들에 관하여 조사한다. 용어는 이론의 개념을 나타내는 매우 긴요한 구성 요소로서 모든 체계에 있어서 용어의 적절한 정의는 필수적이다. 국내에서 SC27과 관련하여 많은 국내 표준화가 이루어지고 있으나, 용어의 선택과 그 정의에 관한 합의는 아직 도출되지 못한 실정이다. 따라서 본고에서는 관련된 영어 정의와 해당되는 한글 정의를 제시함으로써 국내 관련 용어 표준화에 기여하고자 하며, 암호학의 기본적인 개념들을 정립하고자 할 때 정확한 개념의 확립에 도움이 되고자 한다. 본 고는 ISO/IEC JTC1 SC27/WG2의 Editor인 C. J. Mitchell(영국)에 의한 WG2 문서[M1]에 기초하고 있다. 본 고에서는 단지 ISO/IEC JTC1 SC27/WG2의 용어들만을 정의하며, 추후 다른 WG의 용어들의 보강하고, 전문가들의 의견을 종합하여 용어의 국내 표준화를 완성하고자 한다.

1. 서 론

본 고에서는 ISO/IEC JTC1 SC27/WG2의 용어들에 관하여 조사한다. 용어는 이론의 개념을 나타내는 아주 긴요한 구성요소로서 모든 체계에 있어서 용어의 적절한 정의는 필수적이다. 국내에서 SC27과 관련하여 많은 국내 표준화가 이루어지고 있으나, 용어의 선택과 그 정의에 관한 합의는 아직 도출되고 있지 못한 실정이다. 따라서 본고에서는 관련된 영어 정의와 해당되는 한글 정의를 제시함으로써 국내 관련 용어 표준화에 기여하고자 하며, 암호학의 기본적인 개념들을 정립하고자 할 때 정확한 개념의 확립에 도움이 되고자 하는 목적을 가지고 있다. 본 고는 ISO/IEC JTC1 SC27/WG2의 Editor인 C. J. Mitchell(영국)에 의한 WG2 문서[M1]에 기초하고 있다. 본 고에서는 단지 ISO/IEC JTC1 SC27/WG2의 용어들만을 정의하며, 용어의 정의에는 기존의 용어집들도 참고 하였다[M1,S2,S3]. 제 2절에서는 용어들을 정의하고 제 3절에서는 용어의 영어 알파벳 순에 의한 나열과 가나다 순에 의한 나열을 정리한다.

2. 용어들의 정의

용어들의 정의를 나열한다. 영어 용어와 대응되는 한글 용어 및 그 정의 그리고 영어로 표현된 용어의 정의, 그리고 표준 출처를 제시한다.

* 연세대학교
** 광운대학교

accreditation authority : 인가 기관

- 고유 인가 정보의 생성을 목적으로 하는 모든 구성 단위들이 신뢰할 수 있는 실체.
- An entity trusted by all members of a group of entities for the purposes of the generation of private accreditation information.
- [ISO/IEC 1st CD 9798-5 (12/1995)]

accreditation multiplicity parameter : 인가 중복 매개 변수

- 인가 기관이 각 실체들에게 제공하는 비밀 인가 정보 항목들의 수.
- A positive integer equal to the number of items of secret accreditation information provided to an entity by the accreditation authority.
- [ISO/IEC 1st CD 9798-5 (12/1995)]

adjudicator : 판결자

- 증거에 기초하여 논쟁을 해결할 수 있는 판단자 또는 중재자.
- A judge or arbiter capable of resolving disputes based on evidence.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

appendix : 첨가

- 첨가 함수의 결과인 비트 문자열.
- A string of bits, output of an appendix function.
- [ISO/IEC WD 14888-1 (01/1996)]

appendix function : 첨가 함수

- 공개 함수로서 서명, 증거, 그리고 데이타 객체들을 비트 문자열로 변환한다.
- A public function, which transforms the signature and possibly the witness and the data objects to a string of bits.
- [ISO/IEC WD 14888-1 (01/1996)]

assignment : 할당

- 할당 함수의 결과.
- The output of an assignment function.
- [ISO/IEC WD 14888-1 (01/1996)]

assignment function : 할당 함수

- 시스템 변수에 의해 결정되는 함수로서 증거를 필수적인 입력으로 하고 데이타의 일부분도 입력으로 할 수 있는 공개된 함수.
- A public function which is determined by the system parameters and which takes the witness as a mandatory input and a part of the data to be signed as optional input.
- [ISO/IEC WD 14888-1 (01/1996)]

asymmetric cryptographic technique : 비대칭 암호 기술

- 두 개의 관련된 함수, 즉, 공개 키로 정의한 공개 함수와 고유 키로 정의한 고유 함수를 사용하는 암호 기술을 말하며, 이 두 함수는 주어진 공개 함수로 고유 함수를 찾아내는 것이 계산적으로 불가능한 성질을 갖는다.
- A cryptographic technique that uses two related transformations, a public transformation(defined by the public key) and a private transformation(defined by the private key). The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation.
- [ISO/IEC 1st CD 9798-1(01/1996)]

asymmetric encipherment system : 비대칭 암호 시스템

- 암호화 과정에 공개 함수를 사용하고 복호화

과정에 고유 함수를 사용하는 비대칭 기술에 기초한 시스템.
- A system based on asymmetric techniques whose public transformation is used for encipherment and whose private transformation is used for decipherment
- [ISO/IEC 4th CD 11770-3 (12/1995)]

asymmetric key pair : 비대칭 키 쌍

- 고유 함수를 정의하는 고유 키와 공개 함수를 정의하는 공개 키들의 쌍.
- A pair of related keys where the private key defines the private transformation and the public key defines the public transformation.
- [ISO/IEC 4th CD 11770-3 (12/1995)]

asymmetric signature system : 비대칭 서명 시스템

- 고유 함수가 서명을 위해 사용되고 공개 함수가 증명을 위해 사용되어지는 비대칭 기술에 기초한 시스템.
- A system based on asymmetric techniques whose private transformation is used for signing and whose public transformation is used for verification.
- [ISO/IEC 4th CD 11770-3 (12/1995)]

bilateral counter : 쌍방 계수기

- 두 통신 실체들 사이에서 배타적으로 사용되고 관리되는 계수기.
- A counter that is used and managed exclusively between two communicating entities.
- [ISO/IEC 4th CD 11770-3 (12/1995)]

block : 블록

- Lx 비트의 문자열.
- A string of Lx bits.
- [ISO/IEC 3rd CD 10118-3 (04/1996)]

block chaining : 블록 연결

- 암호문의 각 블럭들이 선행하는 암호문 블록들에 암호적으로 관련되도록 하는 정보의 암호화.
- The encipherment of information such that each block of ciphertext is cryptographically dependent upon the preceding ciphertext block.
- [ISO 8372 : 1987, ISO/IEC 1st CD 10116 (12/1995)]

certificate : 인증서

- 인증 기관의 고유 키 또는 비밀 키를 사용하여 변조를 불가능하게 한 실체의 데이타.
- An entity's data rendered unforgeable with the private or secret key of the certification authority.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

certification authority (CA) : 인증 기관

- 공개 키 인증서를 만들고 분배하는 신뢰할 수 있는 기관. 인증 기관은 키들을 만들어서 각 실체에게 분배할 수도 있다.
- A centre trusted to create and assign public key certificates. Optionally, the certification authority may create and assign keys to the entities.
- [ISO/IEC 1st DIS 11770-1 (12/1995), ISO/IEC 4th CD 11770-3 (12/1995)]

challenge : 접속

- 요구자가 사용하는 것으로서, 증명자가 임의로 선택하여 요구자에게 보내는 데이타 항목이다. 이와함께, 요구자는 그것을 비밀 정보로

간직하여, 증명자에게 회답할 때 사용한다.

- A data item chosen at random and sent by the verifier to the claimant, which is used by the claimant, in conjunction with secret information held by the claimant, to generate a response which is sent to the verifier.
- [ISO/IEC 1st CD 9798-5 (12/1995)]

ciphertext : 암호문 (또는 cipher text)

- 정보의 내용을 감추기 위하여 변환된 데이타.
- Data which has been tranformed to hide its information content.
- [ISO/IEC 1st CD 9798-1 (01/1996)]

collision-resistant hash-function : 충돌 회피 해쉬 함수

- 같은 출력을 내는 서로 다른 두 입력을 찾기가 계산적으로 불가능한 성질을 갖는 해쉬 함수.
- A hash-function satisfying the following property :
- it is computationally infeasible to find any two distinct inputs which map to the same output.
- [ISO/IEC 10118-1 : 1994, ISO/IEC WD 14888-3 (01/1996)]

commitment : 실행

- 요구자가 계산해서 검증자에게 보내는 데이타 항목.
- A data item computed by the claimant, and which is sent to the verifer.
- [ISO/IEC 1st CD 9798-5 (12/1995)]

commitment function : 실행 함수

- 임의로 혹은 의사 임의로 생성된 지수를 가지고 서명자가 계산한 지수값을 입력으로 하고, 서명의 첫 부분을 출력으로 하는 함수. 만약 실행 함수가 다른 입력을 갖고 있지 않다면 그것은 형태 1의 실행 함수이며, 그것은 지수를 입력으로 하는 일방향 함수인 형태로 선택되어져야 한다. 형태 2의 실행 함수는 메시지나 다른 객체를 입력으로 한다. 이 경우 실행 함수는
  1. 각각의 고정된 지수에 대하여 메시지의 충돌 회피 해쉬 함수여야 하고,
  2. 각각의 고정된 메시지에 대하여 출력은 지수의 일방향 함수이도록 선택되어야 한다.
- The function which takes as input an exponentiation computed by the signer from a randomly or pseudo-randomly generated exponent, and which gives the first part of the signature as output. If the commitment function does not have other inputs, it is a commitment function of type 1 and it must be chosen in such a way that it is a one-way function of the exponent. A commitment function is of type 2 if it also takes the message and optionally an object as input. In this case the commitment function must be chosen such that for each fixed exponential, it is a collision resistant hash-function of the message, and for each fixed message the output is a one-way function of the exponent.
- [ISO/IEC WD 14888-3 (01/1996)]

cryptographic algorithm : 암호 알고리즘

- 하나 이상의 비밀 매개 변수를 사용하여 데이타의 정보 내용을 숨기거나 찾기 위해 데이타를 변형시키는 알고리즘.
- A cryptographic algorithm is defined as an algorithm which transforms data in order to hide or reveal its information content and which uses at least one secret parameter.

This definition includes both symmetric algorithms(e.g. DES and FEAL) and asymmetric algorithms(e.g. RSA and Rabin). In the case of a symmetric algorithm the data is hidden and revealed using a secret parameter. In the case of an asymmetric algorithm the data is hidden using a public parameter and revealed using a secret parameter.
- [ISO/IEC 9979 : 1991]

cryptographic check function : 암호적 검사 함수

- 비밀 키와 임의의 문자열을 입력으로 하여 암호적 검사값을 출력으로 하는 암호적 변환. 검사값을 위조하기가 계산상 불가능해야 한다.
- A cryptographic transformation which takes as input a secrete key and an arbitrary string, and which gives a cryptographic check value as output. The check value must be infeasible to forge.
- [ISO/IEC 1st CD 9798-1 (01/1996)]

cryptographic check value : 암호적 검사값

- 데이터 단위당 암호적 변환을 실행시켜 유도되는 정보.
- Information which is derived by performing a cryptographic transformation on the data unit.
- [ISO/IEC 9797 (2nd edition): 1994, ISO/IEC 9798-1 : 1995]

cryptographic synchronization : 암호적 동기

- 암호화와 복호화 과정의 상호 조정.
- The co-ordination of the encipherment and decipherment processes.
- [ISO/IEC 1st CD 10116 (12/1995)]

data input : 데이타 입력

- 메시지 함수의 출력.
- The output of a message function.
- [ISO/IEC WD 14888-1 (01/1996)]

data integrity : 데이타 무결성

- 인가되지 않은 방법으로 데이타가 변경되거나 훼손되지 않는 성질.
- The property that data has not been altered or destroyed in an unauthorized manner.
- [ISO/IEC 9797 (2nd edition): 1994]

data object : 데이타 객체

- 서명자와 검증자가 알고 있거나 접근할 수 있는 비트들의 구조화된 문자열.
- A structured string of bits which is known by or accessible to the signer and to the verifier.
- [ISO/IEC WD 14888-1 (01/1996)]

data storage : 데이타 저장

- 전송을 위하여 제출된 데이타 혹은 전송 기관에 의하여 보관된 데이타들의 저장고.
- A container from which data is submitted for delivery, or into which data is put by the delivery authority.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

data string (data) : 데이타 문자열

- 해쉬 함수의 입력으로 사용하는 비트들의 문자열.
- The string of bits which is the input to a hash fnction.
- [ISO/IEC 10118-1 : 1994]

decipherment : 복호화

- 대응되는 암호화 과정의 역과정으로 암호적 알고리즘에 의하여 암호문을 평문으로 대응시키는 변환.
- The reversal of a corresponding reversible encipherment.
- [ISO/IEC 1st CD 9798-1 (01/1996)]

delivery authority : 전송 기관

- 송신자가 수신자에게 데이타를 전달할 때, 송신자가 신뢰할 수 있는 기관으로서 요청이 있을때는 송신자에게 데이타의 제출이나 전송의 증거를 제공할 수 있는 기관이다.
- An authority trusted by the sender to deliver data from the sender to the receiver, and to provide the sender with evidence on the submission and transport of data upon request.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

digital signature : 디지털 서명

- 데이타 단위에 대한 암호적 변환으로 그 데이타의 수신자에게 그 발신과 데이타의 무결성을 증명할 수 있게 하고, 제 3자에 의해 변조된 데이타로 인한 전송자와 수신자의 피해를 예방하고, 수신자의 데이타 변조로 인한 전송자의 피해를 예방할 수 있는 것이다.
- A cryptographic transformation of a data unit that allows a recipient of the data unit to prove the origin and integrity of the data unit and protect the sender and the recipient of the data unit against forgery by the recipient.
- [ISO/IEC1st DIS 11770-1 (12/1995)]

distinguishing identifier : 식별자

- 객체를 명확히 구별하도록 하는 정보.
- Information which unambiguously distinguishes an entity.
- [ISO/IEC 1st CD 9798-1 (01/1996)]

encipherment : 암호화

- 암호문을 만들기 위한, 즉 데이타의 내용을 숨기기 위해 암호적 알고리즘에 의한 데이타 변환을 말함.
- The reversible transformation of data by a cryptographic algorithm to produce ciphertext, i.e. to hide the data.
- [ISO/IEC 1st CD 9798-1 (01/1996)]

entity authentication : 실체 인증

- 어떤 실체가 실체라고 주장하는 합작.
- The corroboration that an entity is the one claimed.
- [ISO/IEC 11770-2 : 1996]

evidence : 증거

- 그 자체로 혹은 다른 정보와 연관하여 어떤 사건이나 행위에 대한 증명을 하는데 사용되는 데이타.
- Information that either by itself or when used in conjunction with other information is used to establish proof about an event or action.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

evidence requester : 증거 요청자

- 다른 실체 혹은 신뢰 받는 제 3자에 의해 생성되어지는 증거를 요청하는 실체.
- An entity requesting an evidence to be generated either by another entity or by a trusted third party.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

exchange multiplicity parameter : 교환 중복 매개 변수

- 실체 인증 메세지의 변환되어야 할 정도를 결정하기 위하여 사용되는 양의 정수.
- A positive integer used to determine how change of entity authentication messages shall be performed.
- [ISO/IEC 1st CD 9798-5 (12/1995)]

feedback buffer : 피드백 버퍼

- 암호화 과정을 위한 입력 데이타를 저장하기 위하여 사용하는 변수.
- Variable used to store input data for the encipherment process.
- [ISO/IEC 1st CD 10116 (12/1995)]

half-block : 반 블록

- LH/2 비트의 문자 열
- A string of LH/2 bits.
- [ISO/IEC 2nd CD 10118-4 (05/1995)]

hash-code : 해쉬 코드

- 해쉬 함수의 출력 비트 문자열.
- The string of bits which is the output of a hash-function.
- [ISO/IEC WD 14888-1 (01/1996)]

hash-function : 해쉬 함수

- 임의의 비트 문자열을 고정된 비트 문자열로 출력하는 함수로서 다음 두가지 성질을 만족한다.
  1. 주어진 출력에 대해 그 입력값을 찾아내기가 계산상 불가능하다.
  2. 주어진 입력에 대해 같은 출력값을 갖는 또 다른 입력값을 찾기가 계산상 불가능하다.
- A function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties.
- it is computationally infeasible to find for a given output an input which maps to this output;
- it is computationally infeasible to find for a given input a second input which maps to the same output.
- [ISO/IEC 1st CD 14888-1 (05/1995)]

identity : 정체성

- 실체에게 할당되고 그것을 동일화하는데 사용되어지는 데이타 항목들의 열.
- A sequence of data items assigned to an entity and used to identify it
- [ISO/IEC 1st CD 9798-5 (12/1995)]

implicit key authentication to A : 객체 A에 대한 감추어진 키 인증

- 단지 동일화 된 다른 실체만이 올바른 키를 가질 수 있는 A에 대한 보증.
- The assurance for one entity A that only another identified entity can(possibly) be in possession of the correct-key.
- [ISO/IEC 4th CD 11770-3 (12/1995)]

initializing value : 초기 값

- 해쉬 함수의 시작을 정의할 때 사용되는 값.
- A value used in defining the starting point of a hash-function
- [ISO/IEC 10118-1 : 1994]

interleaving attack : 인터리빙 공격

- 한번 이상 진행되거나 또는 사전 인증 교환으로부터 유도되는 정보의 사용을 포함하는 위장.
- A masquerade which involves use of information derived from one or more ongoing or previous authentication exchanges.

- [ISO/IEC 1st CD 9798-1 (01/1996)]

key : 키

- 암호적 변환(즉 암호화, 복호화, 암호적 검사 함수 계산, 서명 계산 또는 서명 증명)의 작동을 조절하는 기호들의 열.
- A sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check function computation, signature calculation, or signature verification).
- [ISO/IEC 1st CD 9798-1 (01/1996)]

key agreement : 키 동의

- 실체들에게 공유된 비밀 키를 설정하는 과정으로 각 실체 어느 누구도 미리 그 값을 결정할 수 없다.
- The process of establishing a shared secret key between entities in such a way that neither of them can predetermine its value.
- [ISO/IEC 1st DIS 11770-1 (12/1995)]

key confirmation : 키 확증

- 신원이 밝혀진 다른 실체가 올바른 키를 가지고 있는 한 실체를 보증하는 것.
- The assurance for one entity that another identified entity is in possession of the correct key.
- [ISO/IEC 1st DIS 11770-1]

key control : 키 제어

- 키 계산에 사용되는 변수 혹은 키를 선택하는 능력.
- The ability to choose the key, or the parameters used in the key computation.
- [ISO/IEC 1st DIS 11770-1 (12/1995)]

key distribution centre (KDC) : 키 분배 센터

- KDC와 키를 나누는 각 실체에게 키를 생성 혹은 취득, 그리고 분배하는 신뢰되는 실체.
- An entity trusted to generate or acquire, and distribute keys to entities that each share a key with the KDC.
- [ISO/IEC 1st DIS 11770-1 (12/1995)]

key establishment : 키 설정

- 하나 또는 그 이상의 실체들이 사용할 수 있는 비밀 키를 만드는 과정.
- The process of making available a shared secret key to one or more entities.
- [ISO/IEC 4th CD 11770-3 (12/1995)]

key generating function : 키 생성 함수

- 적어도 한 개는 비밀로 할 수 있는 몇 개의 변수들을 입력으로 하고, 의도한 알고리즘과 응용에 적합한 키를 출력으로 갖는 함수. 이 함수는 비밀 입력에 대한 사전 지식이 없이 출력을 추측해 내는 것이 계산상 불가능한 성질을 가진다.
- A function which takes as input a number of parameters, at least one of which shall be secret, and which gives as output keys appropriate for the intended algorithm and application. The function shall have the property that it is computationally infeasible to deduce the output without prior knowledge of secret input.
- [ISO/IEC 11770-2: 1996]

key generation exponent : 키 생성 지수

- 비밀 시스템 변수로서 신뢰 기관만이 알고 있는 정수 값이다.
- A serete system parameter, an integer known only to the trusted authority.

- [ISO/IEC WD 14888-2 (01/1996)]

key management : 키 관리

- 보안 정책에 의해 키의 생성, 등록, 인가, 등록취소, 분배, 설치, 저장, 압축, 폐지, 유도와 파괴를 감독하는 것.
- The administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation and destruction of keying material in accordance with a security policy.
- [ISO/IEC 1st DIS 11770-1 (12/1995)]

key token : 키 토큰

- 키 관리 메카니즘을 실행하는 동안 한 실체가 다른 실체에게 보내는 키 관리 메시지.
- Key managemenat message sent from one entity to another entity during the execution of a key management mechanism.
- [ISO/IEC 1st DIS 11770-1 (12/1995)]

key translation centre (KTC) : 키 변환 센터

- KTC와 키를 나누어 갖고 있는 각 실체들 사이에 키 변환 임무를 수행하는 실체들이 신뢰할 수 있는 실체.
- An entity trusted to translate keys between entities that each share a key with the KTC.
- [ISO/IEC 1st DIS 11770-1 (12/1995)]

key transport : 키 전송

- 한 실체가 다른 실체에게 키를 적절히 보호한 상태로 보내는 과정.
- The process of transferring a key from one entity to another entity, suitably protected.
- [ISO/IEC 4th CD 11770-3 (12/1995)]

keying material : 키 요소

- 암호적인 키 관계를 만들거나 유지시키기 위해 필요한 자료.
- The data (e.g. keys, initialization values) necessary to establish and maintain cryptographic keying relationship.
- [ISO/IEC 1st DIS 11770-1 (12/1995)]

masquerade : 위장

- 한 실체가 다른 실체처럼 흉내내는 것.
- The pretence by an entity to be a different entity.
- [ISO/IEC WD 9798-1 (05/1995)]

message : 메시지

- 제한된 길이를 가지는 문자열.
- String of bits of limited length. String of bits of any length.
- [ISO/IEC WD 9796-2 (01/1996)]

message function : 메시지 함수

- 메시지와 선택된 데이타 객체를 입력으로 하고, 그것들을 증거와 할당 함수에 대한 입력으로 준비해 두는 공개된 함수.
- A public function which takes the message and optional data objects as inputs and prepares them for input to the witness and assignment functions.
- [ISO/IEC WD 14888-1 (01/1996)]

message authentication code : 메시지 인증 코드

- 데이타 무결성 메카니즘에서 쓰이는 암호적 검사값
- A cryptograpic check value used in a data integrity mechanism.

- [ISO/IEC 1st DIS 11770-2 (12/1994)]

modulus : 법

- 서로 다른 홀수인 두 소수의 곱으로 표현되는 양의 정수.
- A positive integer equal to the product of two distinct odd prime numbers.
- [ISO/IEC 5th WD 9798-5 (05/1995)]

mutual authentication : 상호 인증

- 두 실체에게 상대방의 신분을 확인시켜주는 실체 인증.
- Entity authentication which provides both entities with assurance of each other's identity.
- [ISO/IEC 1st CD 9798-1 (01/1996)]

n-bit block cipher algorithm : n 비트 블럭 암호 알고리즘

- 평문 블럭과 암호문 블럭의 길이를 각각 n으로 하는 블럭 암호 알고리즘.
- A block cipher algorithm with the property that plaintext blocks and ciphertext blocks are n bits in length.
- [ISO/IEC 10118-2: 1994, ISO/IEC 9797 (2nd EDITION): 1994, ISO/IEC 1st CD 10116 (12/1995)]

non-repudiation certificate : 부인 봉쇄 인증서

- 어떤 행위 또는 사건에 관련된 실체의 자료로서 그 행위 또는 사건과 연관하여 반증할 수 없는 증거로 사용할 수 있으며 그 증거는 변조가 불가능하다. 이 인증서를 제 3의 신뢰기관이 비밀 키를 사용하여 안전한 문서 형태로 실체들에게 제공하기도 하며, 부인 봉쇄 회원들은 각자의 공개 키 인증서와 연관시켜 자기의 고유 키로 전자 서명을 할 수 있다.
- A special type of security certificate as defined in ISO/IEC 10181-1 which constitutes an evidence, and is used by a non-repudiation service to validate an evidence.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

non-repudiation exchange : 부인 봉쇄 교환

- 부인 봉쇄를 목적으로 부인 봉쇄 정보를 보내는 일련의 과정.
- A sequence of one or more transfers of non-repudiation information (NRI) for the purpose of non-repudiation.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

non-repudiation information : 부인 봉쇄 정보

- 사건 또는 행위와 관련하여 그 증거가 유효하고, 그 증거 자체와 부인 봉쇄 정책이 유효함을 보여줄 수 있도록 만든 정보들의 집합.
- A set of information that may consist of the information about an event or action for which evidence is to be generated and validated, the evidence itself, and the non-repudiation policy in effect.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

non-repudiation of approval : 승인 부인 봉쇄

- 이 서비스는, 수신자가 메시지의 내용을 승인했었던 사실을 거짓 부인하지 못하도록 하려는 것이다.
- This service is intended to protect against an entity's false denial of having approved the content of a message(i.e. being responsible for the content of a message).
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

non-repudiation of delivery : 전송 부인 봉쇄

- 이 서비스는, 수신자가 메시지를 전달받았음

과 메시지 내용을 인정했었음을 거짓 부인하지 못하도록 하려는 것이다.
- This service is intended to protect against a recipient's false denial of having received the message and recognized the content of a message.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

non-repudiation of knowledge : 인지 부인 봉쇄

- 이 서비스는, 수신자가 수신된 메시지 내용을 알고 있음을 거짓 부인하지 못하도록 하는 것이다.
- This service is intended to protect against a recipient's false denial of having recognized the content of a received message.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

non-repudiation of origin : 출처 부인 봉쇄

- 이 서비스는, 객체가 어떤 메세지를 처음 생성했을 때, 그 사실을 부인하지 못하도록 하는 것이다.
- This service is intended to protect against the originator's false denial of having approved the content of a message and of having sent a message.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

non-repudiation of receipt : 수신 부인 봉쇄

- 이 서비스는, 수신자가 메시지를 수신했음을 거짓 부인하지 못하도록 하는 것이다.
- This service is intended to protect against a recipient's false denial of having received a message.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

non-repudiation of sending : 송신 부인 봉쇄

- 이 서비스는, 송신자가 메시지를 송신했음을 거짓 부인하지 못하도록 하는 것이다.
- This service in intended to protect against the sender's false denial of having sent a message.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

non-repudiation of submission : 제출 부인 봉쇄

- 이 서비스는, 전송 기관이 전송될 메시지를 받았었음을 거짓 부인하지 못하도록 하는 것이다.
- This service is intended to protect against a delivery authority's false denial of having accepted the message for transmission.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

non-repudiation of transport : 전송 부인 봉쇄

- 이 서비스는, 전송 기관이 메시지를 요구자의 자료 저장소에 정확히 전달했음을 거짓 부인하지 못하도록 하는 것이다.
- This service is intended to protect against a delivery authority's false denial of having delivered the message into the data storage of the intended recipient.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

non-repudiation policy : 부인 봉쇄 정책

- 부인 봉쇄 서비스를 제공할 때 필요한 일련의 판단 기준을 말한다. 세부적으로 증거의 생성과 증명 그리고 판결에 필요한 일련의 규칙을 말한다.
- A set of criteria for the provision of non-repudiation services. More specifically, a set of rules to be applied for the generation and verification of evidence and for adjudication.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

non-repudiation token : 부인 봉쇄 토큰

- 부인 봉쇄 정보를 전달할 때 쓰이는 부인 봉

쇄 증명서와 부수적인 정보등 일련의 자료를 말한다. 이것은 회원들이나 제 3의 신뢰기관이 만들 수 있으며 논쟁이 생길 경우에 대비해 증거로 남겨둔다.
- A special type of security token as defined in ISO/IEC 10181-1 consisting of a set of evidence and, optionally, of additional data.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

NRD token : NRD 토큰

- 전송 부인 봉쇄 토큰. 메시지 출처자로 하여금 메시지 전송 부인을 봉쇄하기 위하여 필요한 자료들이다.
- Non-repudiation of delivery token. A data item which allows the originator to establish non-repudiation of delivery for a message.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]
- [ISO/IEC/JTC1/SC27/WG2 Terminology (04/96)]

- Non-repudiation of delivery token. A data field which allows the originator to establish non-repudiation of delivery for a message.
- [ISO/IEC 1st CD 13888-3 (09/1995)]

NRO token : NRO 토큰

- 출처 부인 봉쇄 토큰. 메시지 수신자들로 하여금 메시지 출처 부인을 봉쇄하기 위하여 필요한 자료들이다.
- Non-repudiation of origin token. A data item which allows recipients to establish non-repudiation of origin for a message.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

- Non-repudiation of origin token. A data field which allows the recipient to establish non-repudiation of origin for a message.
- [ISO/IEC 1st CD 13888-3 (09/1995)]

NRS token : NRS 토큰

- 제출 부인 봉쇄 토큰. 메시지 출처자가 전송한 메시지에 대해 전송 부인을 봉쇄하기 위하여 필요한 자료들이다.
- Non-repudiation of submission token. A data item which allows either the originator (sender) or the delivery authority to establish non-repudiation of submission for a message having been submitted for transmission.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

- Non-repudiation of submission token. A data field which allows the originator to establish non-repudiation of submission for a message having been submitted for transmission.
- [ISO/IEC 1st CD 13888-3 (09/1995)]

NRT token : NRT 토큰

- 전송한 사실을 부인하지 못하게 하기 위한 자료들이다.
- Non-repudiation of transport token. A data item which allows either the originator or the delivery authority to establish non-repudiation of transport for a message.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

- Non-repudiation of transport token. A data field which allows the delivery authority to establish non-repudiation of transport for a message.
- [ISO/IEC 1st CD 13888-3 (09/1995)]

one-way function : 일방향 함수

- 함수값 계산은 쉬우나, 함수값으로부터 역상을 찾아내기가 계산상 불가능한 함수.

- A function which is easy to compute but whose inverse is computationally intractable.
- [ISO/IEC 4th CD 11770-3 (12/1995), ISO/IEC WD 14888-3 (01/1996)]

originating entity : 근본 실체

- 부인 봉쇄가 된 사건 또는 행위에 연루된 실체.
- The entity that is concerned by the event or action that becomes non-repudiable.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

originator : 출처자

- 부인 봉쇄 서비스가 제공되는 메시지를 사용할 수 있거나 요구자에게 전달하는 객체.
- The entity that sends a message to the recipient or makes available a message for which non-repudiation services are to be provided.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]
- [ISO/IEC/JTC1/SC27/WG2 Terminology (04/96)]

- The entity that sends a message to the recipient for which non-repudiation services are to be provided.
- [ISO/IEC 1st CD 13888-3 (09/1995)]

padding : 덧붙이기

- 데이타 문자열에 부가적인 비트들을 덧붙이는 것.
- Appending extra bits to a data string.
- [ISO/IEC 10118-1 : 1994]

plaintext : 평문

- 암호화되지 않은 정보.
- Unenciphered information.
- [ISO 8372 : 1987, ISO/IEC 1st CD 10116 (12/1995)]

point-to-point key establishment : 일대일 키 설정

- 제 3의 객체를 통하지 않고 실체 사이에서 키를 직접적으로 설정하는 것.
- The direct establishment of keys between entities, without involving a third party.
- [ISO/IEC 11770-2 : 1996]

pre-signature : 예비 서명

- 예비 서명 함수의 결과.
- The output of a pre-signature function.
- [ISO/IEC WD 14888-1 (01/1996)]

pre-signature function : 예비 서명 함수

- 서명 과정에서 쓰이는 함수로서, 시스템 매개 변수들과 될 수 있다면 서명 키를 이용해 그 함수를 결정할 수 있으며, 실행을 입력으로 하고, 예비 서명을 출력으로 한다.
- A function in the signature process, which is determined by the system parameters and possibly the signature key, takes the commitment as input and gives the pre-signature as output.
- [ISO/IEC WD 14888-1 (01/1996)]

private accreditation information : 고유 인가 정보

- 인가 기관이 요구자에게 제공하는 고유 정보를 말하며, 요구자는 그 정보를 알고 있음을 증명함으로서 자신의 신분을 확인시킬 수 있다.
- Private information provided to a claimant by an accreditation authority, and of which a claimant proves knowledge, thereby establishing the claimant's identity.

- [ISO/IEC 1st CD 9798-5 (12/1995)]

private decipherment transformation : 고유 복호화 함수

- 비대칭 암호화 시스템과 비대칭 키 쌍의 고유 키에 의해 결정된 복호화 함수.
- The decipherment transformation determined by an asymmetric encipherment system and a private key of an asymmetric key pair.
- [ISO/IEC 1st CD 9798-5 (12/1995)]

private key : 고유 키

- 한 실체의 비대칭 키 쌍중에서 그 실체만이 사용하는 키를 말한다. 비대칭 서명 시스템에서 서명 함수를 정의할 때 사용된다.
- That key of an entity's asymmetric key pair which should only be used by that entity. In the case of an asymmetric signature system, the private key defines the signature transformation.
- [ISO/IEC 1st DIS 11770-1 (12/1995)]
- [ISO/IEC/JTC1/SC27/WG2 Terminology (04/96)]

- That key of an entity's asymmetric key pair which should only be used by that entity.
- [ISO/IEC 4th CD 11770-3 (12/1995)]

- That key of an entity's asymmetric key pair which is usable only by that entity. In the case of an asymmetric signature system, the private key and associated algorithms define the signature transformation.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

private signature exponent : 고유 서명 지수

- 인증 기관만이 알고있는 값으로서, 요구자의 고유 인증 정보를 생성할 때 쓰인다.
- A value known only to the accreditation authority, and which is used in the production of claimant's private accreditation information.
- [ISO/IEC 1st CD 9798-5 (12/1995)]

private signature key : 고유 서명 키

- 고유 서명 함수를 정의할 때 쓰는, 한 실체의 비대칭 키 쌍
- The key of an entity's asymmetric key pair which defines the private signature transformation.
- [ISO/IEC 1st CD 9798-1 (01/1996)]

proof : 증명

- 보강 증거로서, 사실상 특별한 부인 봉쇄 정책과 일치하는 (필요하고도 충분한) 정보를 나타내는 증거.
- The corroboration that the evidence represents the (necessary and sufficient) information that matches the particular non-repudiation policy in effect.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

public encipherment transformation : 공개 암호화 함수

- 비대칭 암호화 시스템과 비대칭 키 쌍중에서 공개 키로 결정되는 암호화 함수
- The encipherment transformation determined by an asymmetric enci-pherment system and a public key of an asymmetric key pair.
- [ISO/IEC 1st CD 9798-5 (12/1995)]

public key : 공개 키

- 한 실체의 비대칭 키 쌍중에서 공개되는 키를 말한다. 비대칭 서명 시스템에서 증명 함수를 정의할 때 사용된다.
- That key of an entity's asymmetric key pair which can be made public. In the case of an asymmetric signature system the public key defines the verification transformation.
- [ISO/IEC 1st DIS 11770-1 (12/1995)]

- That key of an entity's asymmetric key pair which can be made public.
- [ISO/IEC/JTC1/SC27/WG2 Terminology (04/96)]

- That key of an entity's key pair which can be made public. In the case of an asymmetric signature system, the public key and the associated algorithms define the verification transformation.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

public key certificate : 공개 키 인증서

- 한 실체의 공개 키에 관한 정보로서 인증 기관이 서명한 것을 말하며, 서명으로 인해 변조가 불가능한 것이다.
- The public key information of an entity signed by the certification authority and thereby rendered unforgeable.
- [ISO/IEC 1st CD 9798-1 (01/1996), ISO/IEC 1st DIS 11770-1 (12/1995), ISO/IEC 4th CD 11770-3 (12/1995)]

- A security certificate which binds unforgeable the public key of an entity with the entity's distinguishing identifier by a certification authority.
- [ISO/IEC 3rd CD 13888-1 (01/1996)]

public key function : 공개 키 함수

- 서명자의 정체성을 서명자의 공개 증명 키로 변환시켜 주는 공개 함수
- A public function which transforms the signer's identity to the signer's public verification key.
- [ISO/IEC WD 14888-2 (01/1996)]

public key information : 공개 키 정보

- 적어도 실체의 식별자와 공개 키를 포함하는 정보. 공개 키 정보는 한 실체에 대한 데이타와 이 실체를 위한 공개 키로 제한되며 인증 기관, 실체, 공개키, 또는 관련된 알고리즘에 관한 다른 정적인 정보일 수도 있다.
- Information containing at least the entity's distinguished identifier and public key. The public key information contains data regarding one entity and at least one public key for this entity. There may be other static information regarding the certification authority, the entity, the public key, or the involved algorithms, included in the public key information.
- [ISO/IEC 1st CD 9798-1 (01/1996)]

- Information containing at least the entity's distinguished identifier and public key. The public key information is limited to data regarding one entity, and one public key for this entity. There may be other static information regarding the certification authority, the entity, the public key, or the involved algorithms, included in the public key information.
- [ISO/IEC 4th CD 11770-3 (12/1995)]

public verification key : 공개 증명 키

- 공개 증명 함수를 정의하는 실체의 비대칭

키 쌍.
- The key of an entity's asymmetric key pair which defines the public verification transformation.
- [ISO/IEC 1st CD 9798-1 (01/1996)]

- A key which corresponds to an entity's secret signature key and which is used in the verification process. This key of an entity's asymmetric key pair can be made public.
- [ISO/IEC WD 14888-3 (01/1996)]

random number : 난수

- 값을 예측할 수 없는 수
- A number whose value is unpredictable.
- [ISO/IEC 1st DIS 11770-1 (12/1995)]

- A time variant parameter whose value is unpredictable.
- [ISO/IEC 1st CD 9798-1 (01/1996), ISO/IEC 11770-2 : 1996]

recipient : 수신자

- 부인 봉쇄 서비스가 제공되는 메시지를 수신하는 실체
- The entity that gets (receives or fetches) a message for which non-repudiation services are to be provided.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

- The entity that receives message for which non-repudiation services are to be provided.
- [ISO/IED 1st CD 13888-3 (09/1995)]

reduction function : 감소 함수

- 실행 함수의 출력을 제한된 크기의 양의 정수로 보내는 함수. 감소 함수는 몇몇 객체를 입력으로 가질 수도 있으며 실행 함수와 감소 함수의 합성 함수가 실행 함수의 요구 조건을 만족하도록 선택되어야 한다.
- The function which maps the output of the commitment function to a positive integer of limited size. The reduction function may also take some object as input. The reduction function must be chosen in such a way that the composition of the commitment function and the reduction function satisfies the requirements of a commitment function.
- [ISO/IEC WD 14888-3 (01/1996)]

redundancy: 잉여 정보

- 알려져서 확인될 수 있는 정보.
- Any information that is known and can be checked.
- [ISO/IEC 11770-2 : 1996]

redundant hash-function : 잉여 해쉬 함수

- 입력은 먼저 ISO/IEC 9796에서 정의된 잉여 함수를 거치고, 출력이 1 이상 p-1 이하의 정수 값으로 하는 해쉬 함수
- A hash function where the input is first subjected to the ISO/IEC 9796 redundancy function, and where the output, when regarded as an integer, lies strictly between 0 and P.
- [ISO/IEC WD 14888-3 (01/1996)]

redundant identity : 잉여 정체성

- ISO/IEC 9796에서 기술된 방법을 사용하여, 실체의 정체성에 잉여 정보를 추가하여 얻어지는 데이타 항목의 수열.
- A sequence of data items obtained from an entity's identity by adding redundancy using techniques specified in ISO/IEC 9796.

- [ISO/IEC 1st CD 9798-5 (12/1995)]

reflection attack : 반사 공격

- 이전에 전송된 메시지를 그 메시지 송신자에게 되돌려 보내는 방법을 사용한 위장.
- A masquerade which involves sending a previously transmitted message back to its originator.
- [ISO/IEC 1st CD 9798-1 (01/1996)]
- [ISO/IEC/JTC1/SC27/WG2 Terminology (04/96)]

replay attack : 반복 공격

- 이전에 전송된 메시지를 다시 사용하는 위장.
- A masquerade which involves the use of previously transmitted messages.
- [ISO/IEC 1st CD 9798-1 (01/1996)]

response : 회신

- 요구자가 증명자에게 보내는 데이타 항목으로서, 증명자는 요구자의 정체성을 검토하기 위해 사용할 수 있다.
- A data item sent by the claimant to the verifier, and which the verifier can process to help check the identity of the claimant.
- [ISO/IEC 1st CD 9798-5 (12/1995)]

round-function : 라운드 함수

- 함수 $\phi(...)$은 길이가 L_1이고 L_2인 두 이진스트링을 길이가 L_2인 이진 스트링으로 변환한다. 이것이 해쉬 함수의 일부로써 반복해서 사용되면 길이 L_1인 데이터 블록과 길이 L_2인 이전의 출력을 결합한다.
- A function $\phi(...)$ that transforms two binary strings of lengths L_1 and L_2 to a binary string of length L_2. When used iteratively as a part of a hash-function, the round-function ϕ combines a data string of length L_1 with the previous output of length L_2.
- [ISO/IED 3rd CD 10118-3 (04/1996)]

- A function $\phi(...)$ that transforms two binary strings of lengths L_X and L_Y to a binary string of length L_Y. When used iteratively as a part of a hash-function, the round-function ϕ combines a data string of length L_X with the previous output of length L_Y.
- [ISO/IEC 2nd CD 10118-4 (05/1995)]

secret key : 비밀 키

- 대칭 암호 기술에 사용되며 정해진 실체들에 의해서만 사용되는 키.
- A key used with symmetric cryptographic techniques and usable only by a set of specified entities.
- [ISO/IEC 1st DIS 11770-1 (12/1995), ISO/IEC 4th CD 11770-3 (12/1995)]

- A key used with symmetric cryptographic techniques and used only by a set of specified entities.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

secret signature key : 비밀 서명 키

- 비밀 서명 함수를 정의하는 실체의 비대칭 키 쌍
- The key of an entity's asymmetric key pair which defines the private signature transformation.
- [ISO/IEC WD 14888-3 (01/1996)]

security authority : 보호 기관

- 보호 영역 내에서 보호관련 내용을 다루는 궁극적 기관.

- The ultimate authority for security concerns within a security domain.
- [ISO/IEC 3rd CD 11770-1 (05/1995)]

security domain : 보호 영역

- 보호 정책이 정의된 유효한 영역이며 한 영역을 다른 영역의 요소로 하는 것에 의하여 계층적으로 구성할 수 있다.
- A domain for which a security policy is defined and valid : security domains may be ordered hierarchically by permitting one domain to be a member of another domain.
- [ISO/IEC 3rd CD 11770-1 (05/1995)]

secure envelope (SENV) : 안전 봉투

- 제 3의 신뢰 기관이 무결성과 출처를 증명할 수 있도록 구성한 데이타 항목들의 집합.
- A set of data items which is constructed by a trusted third party (TTP) in such a way that this TTP can verify their integrity and origin.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

signature : 서명

- 서명 과정으로부터 생긴 비트들의 문자열.
- String of bits resulting from the signature process.
- [ISO/IEC 9796: 1991, ISO/IEC WD 9796-2 (01/1996)]
- The output from the signature function.
- [ISO/IEC WD 14888-1 (01/1996)]

signature equation : 서명 방정식

- 서명 함수의 음적인 형태.
- An implicit form of the signature function.
- [ISO/IEC WD 14888-1 (01/1996)]
- $AX+BX+C=0 \bmod Q$
- [ISO/IEC WD 14888-3 (01/1996)]

signature function : 서명 함수

- 서명 키와 시스템 매개 변수들로 결정되고 서명 과정에서 쓰이는 함수를 말한다. 서명 함수는 할당, 그리고 가능하다면 실행을 입력으로 하고 서명을 출력으로 한다.
- A function in the signature process which is determined by the signature key and the system parameters. A signature function takes the assignment and possibly the commitment as inputs and gives the signature as output.
- [ISO/IEC WD 14888-1 (01/1996)]

signature key : 서명 키

- 어떤 한 실체에 한정된 데이타 원소로서 정해진 그 실체만이 서명 과정에서 사용할 수 있다.
- A data element specific to an entity and usable only by this entity in the computation of the signature function.
- [ISO/IEC WD 14888-1 (01/1996)]

signature process : 서명 과정

- 서명할 메시지, 서명키, 시스템 매개 변수와 자료들을 입력으로 하고, 서명된 메시지를 결과값으로 하는 과정.
- A process which takes as inputs the datato be signed, the signature key, the system parameters and an optional data object, and which gives as output the signed message.
- [ISO/IEC WD 14888-1 (01/1996)]

signed message : 서명된 메시지

- 메시지, 서명, 그리고 선택적으로 택한 자료들을 연접시켜 만든 비트들의 문자열.

- The string of bits formed by concatenating the message and the appendix.
- [ISO/IEC WD 14888-1 (01/1996)]

signer : 서명자

- 디지털 서명을 한 실체.
- The entity generating a digital signature.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

starting variable (SV) : 초기 변수

- 초기값에서 유도되는 변수이며, 연산 모드들의 초기점을 정의하는 데 사용된다.
- Variable derived from the initializing value and used in defining the starting point of the modes of operation.
- [ISO 8372: 1987, ISO/IEC 1st CD 10116 (12/1995)]

symmetric cryptographic technique : 대칭 암호 기술

- 송신자와 수신자 모두 같은 비밀 키를 사용하는 암호 기술. 비밀 키를 모르면 송신자 또는 수신자의 전송 메시지를 계산해내는 것은 계산적으로 불가능하다.
- A cryptographic technique that uses the same secret key for both the originator's and recipient's transformation. Without knowledge of the secret key, it is computationally infeasible to compute either the originator's or recipient's trnasformation.
- [ISO/IEC 1st CD 9798-1 (01/1996), ISO/IEC 1st DIS 11770-1 (12/1995)]

symmetric encipherment algorithm : 대칭 암호화 알고리즘

- 대칭 암호 기술을 사용하는 암호화 알고리즘.
- An encipherment algorithm that uses the same secret key for both the originator's and the recipient's transformation.
- [ISO/IEC 1st CD 9798-1 (01/1996)]

system parameter : 시스템 매개 변수

- 시스템내에서 모든 실체에게 공통되고 접근 가능하거나, 알려진 데이타 원소.
- A data element which is common to and known by or accessible to all entities within the system.
- [ISO/IEC WD 14888-1 (01/1996)]

system verification exponent : 시스템 증명 지수

- 정수로서 공개 시스템 매개 변수.
- A public system parameter, an integer.
- [ISO/IEC WD 14888-2 (01/1996)]

time stamp : 시각 소인

- 공통적으로 참고하는 시간에 대해 시간의 기점을 표시하는 시간 변위 매개 변수.
- A time variant parameter which denotes a point in time with respect to a common time reference.
- [ISO/IEC 1st CD 9798-1 (01/1996)]

- A data item which denotes a point in time with respect to a common time reference.
- [ISO/IEC 1st DIS 11770-1 (12/1995)]

time variant parameter : 시간 변위 매개 변수

- 메시지가 난수나, 순번, 시각 소인과 같이 반복되지 않음을 증명하기 위해 실체가 사용하는 데이타 항목.
- A data item used by an entity to verify that a message is not a replay such as a random number, a sequence number, or a time stamp.

- [ISO/IEC 1st CD 9798-1 (01/1996)]

- A data item used to verify that a message is not a replay, such as a random number, a sequence number, or a time stamp.
- [ISO/IEC 1st DIS 11770-1 (12/1995), ISO/IEC 11770-2 : 1996]

token : 토큰

- 특별한 의사소통과 관련된 데이터 구조이며 암호 기술을 사용하여 전송되어진 정보를 포함한다.
- A data field relevant to a particular communication and which contains information that has been transformed using a cryptographic technique.
- [ISO/IEC 1st CD 9798-1 (01/1996)]

trapdoor one-way function : 트랩도어 일방향 함수

- 함수의 값을 계산하기는 쉬우나, 그것의 역은 비밀 트랩도어 정보를 모르면 계산적으로 다루기 불가능한 함수.

trusted third party : 제 3의 신뢰 기관

- 보호 관련 활동에 관하여 다른 실체들이 신뢰하는 보호 기관 또는 그것의 대행 기관. 국제 표준의 문헌에 의하면, 제 3의 신뢰 기관은 인증을 위하여 주장자와/또는 증명자가 신뢰할 수 있는 기관이다.
- A security authority, or its agent, trusted by other entities with respect to security related activities. In the context of this multipart standard, a trusted third party is trusted either by the originator, the recipient, and/or the delivery authority for the purposes of non-repudiation, and by another party such as the adjudicator.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

trusted time stamping authority : 신뢰할 수 있는 시각 소인 기관

- 안전한 시각 소인을 생성할 때 시간을 포함하는 증거를 제공하는 제 3의 신뢰 기관.
- A trusted third party trusted to provide evidence which includes the time when the secure time stamp is generated.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

unilateral authentication : 일방 인증

- 다른 실체의 정체성에 대한 확신을 한 실체에게 제공하는 실체 인증이며, 반대로 상대 실체에게는 그 실체의 정체성에 대한 확신을 제공하지 않는다.
- Entity authentication which provides one entity with assurance of the other's identity but not vice versa.
- [ISO/IEC 1st CD 9798-1 (01/1006)]

verification exponent : 증명 지수

- 실체들의 구성원이 동의한 값으로서 법과 관련하여 고유 서명 지수의 값을 결정한다.
- A value agreed by an members of a group of entities, and which, in conjunction with the modulus, determines the value of the private signature exponent.
- [ISO/IEC 1st CD 9798-5 (12/1995)]

verification function : 증명 함수

- 증명 과정에서 증명 키로 결정되는 함수로서, 증거를 다시 계산한 값을 출력으로 한다.
- A function in the verification process which is determined by the verification key and which gives a recomputed value of the witness as output.

- [ISO/IEC WD 14888-1 (01/1996)]

verification key : 증명 키

- 암호적 검사값 또는 부인 봉쇄 인증서를 증명할 때 필요한 값.
- A value required to verify a cryptographic check value or non-repudiation certificate.
- [ISO/IED 3rd CD 13888-1 (03-1996)]

- A data element which is mathematically related to an entity's signature key and which is used by the verifier in computation of the verification function.
- [ISO/IEC WD 14888-1 (01/1996)]

verification process : 증명 과정

- 서명된 메시지, 증명 키 그리고 시스템 매개변수를 입력으로 하고, 유효하든 하지 않든 서명의 증명 결과를 출력으로 하는 과정.
- A process which takes as input the signed message, the verification key and the system parameters, and which gives as output the result of the signature verification : valid or invalid.
- [ISO/IEC WD 14888-1 (01-1996)]

verifier : 증명자

- 증거를 증명하는 실체.
- An entity that verifies an evidence.
- [ISO/IEC 3rd CD 13888-1 (03/1996)]

witness : 증거

- 증명자가 계산한 데이타 항목으로서 요구자에게 보내진다.
- A data item computed by the verifier, and which is sent to the claimant.
- [ISO/IEC 1st CD 9798-5 (12/1995)]

- The output from a witness function.
- [ISO/IEC WD 14888-1 (01/1996)]

witness function : 증거 함수

- 공개 시스템 매개 변수가 결정하는 공개 함수로서 예비 서명을 필수 입력으로 하고 서명될 데이타의 일부분을 선택 입력으로 한다.
- A public function which is determined by the public system parameters and which takes the pre-signature as a mandatory input and a part of the data to be signed as optional input.
- [ISO/IEC WD 14888-1 (01/1996)]
- ISO/IEC/JTC1/SC27/WG2 Terminology (04/96)

word : 워드

- 32 비트의 문자 열.
- A string of 32 bits.
- [ISO/IEC 3rd CD 10118-3 (04/1996)]

제 3 절 용어의 나열

본 절에서는 앞서 정의된 용어들의 찾아보기를 위한 가나다순 및 알파벳 순의 나열을 한다.

3.1 한글 용어 중심의 가나다 순 나열

감소 함수 reduction function

객체 A에 대한 감추어진 키 인증
implicit key authentication to A

고유 복호화 함수
private signature exponent

고유 서명 지수
private signature exponent

고유 서명 키 private signature key

고유 인가 정보 private accreditation information

고유 키 private key

공개 암호화 함수 public encipherment transformation

공개 키 public key

공개 증명 키 public verification key

공개 키 인증서 public key certificate

공개 키 정보 public key information

공개 키 함수 public key function

교환 곱 매개 변수 exchange multiplicity parameter

근본 실체 originating entity

난수 random number

대칭 기술 symmetric technique

대칭 암호 기술 symmetric cryptographic technique

대칭암호화 알고리즘 symmetric encipherment algorithm

덧붙이기 padding

데이타 객체 data object

데이타 무결성 data integrity

데이타 문자열 data string(data)

데이타 입력 data input

데이타 저장 data storage

디지털 서명 digital signature

라운드 함수 round-function

메시지 message

메시지 인증 코드 message authentication code

메시지 함수 message function

반복 공격 replay attack

반 블록 half-block

반사 공격 reflection attack

법 modulus

보호 기관 security authority

보호 영역 security domain

복호화 decipherment

부인 봉쇄 교환 non-repudiation exchange

부인 봉쇄 인증서 non-repudiation certificate

부인 봉쇄 정보 non-repudiation information

부인 봉쇄 토큰 non-repudiation token

블록 block

블록 연결 block chaining

비대칭 서명 시스템 asymmetric signature system

비대칭 암호 기술 asymmetric cryptographic technique

비대칭 암호화 시스템 asymmetric encipherment system

비대칭 키 쌍 asymmetric key pair

비밀 서명 키 secret signature key

비밀 키 secret key

서명 signature

서명 과정 signature process

서명된 메시지 signed message

서명 방정식 signature equation

서명자 signer

서명 키 signature key

송신 부인 봉쇄
non-repudiation of sending

수신 부인 봉쇄
non-repudiation of receipt

수신자 recipient

승인 부인 봉쇄
non-repudiation of approval

시각 소인 time stamp

시각 변위 매개 변수
time variant parameter

시스템 매개 변수 system parameter

시작 변수 starting variable(SV)

식별자 distinguishing identifier

실체 인증 entity authentication

실행 commitment

실행 함수 commitment function

쌍방 계수기 bilateral counter

안전 봉투 secure envelope(SENV)

암호문 ciphertext, cipher text

암호 알고리즘 cryptographic algorithm

암호적 검사값
cryptographic check value

암호적 검사 함수
cryptographic check function

암호적 동기
cryptographic synchronization

암호화 encipherment

n비트 블럭 암호 알고리즘
n-bit block cipher algorithm

NRD 토큰 NRD token

NRS 토큰 NRS token

NRT 토큰 NRT token

예비 서명 pre-signature

예비 서명 함수 pre-signature function

운반 부인 봉쇄
non-repudiation of transport

워드 word

위장 masqrerade

인가 기관 Accreditation Authority

인가 증복 매개 변수
accreditation multiplicity parameter

인증 기관
Certification Authority(CA)

인증서 certificate

인지 부인 봉쇄
non-repudiation of knowledge

인터리빙 공격 interleaving attack

일대일 키 설정
point-to-point key establishment

일방 인증 unilateral authentication

일방향 함수 one-way function

잉여 정보 redundancy

잉여 정체성 redundant identity

잉여 해쉬 함수 redundant hash-function

전송 기관 delivery authonity

전송 부인 봉쇄
non-repudiation of delivery

접속 challenge

정체성 identity

제출 부인 봉쇄
non-repudiation of submission

증거	evidence
증거	witness
증거 요청자	evidence requester
증거 함수	witness function
증명	proof
증명 과정	verification process
증명자	verifier
증명 지수	verfication exponent
증명 키	verfication key
증명 함수	verfication function
첨가	appendix
첨가 함수	appendix function
초기 값	initializing value
출처 부인 봉쇄	non-repudiation of origin
출처자	originator
충동 회피 해쉬 함수	collision-resistant hash-function
키	key
키 관리	key management
키 동의	key agreement
키 번역 센터	key translation centre(KTC)
키 분배 센터	key distribution center(KDC)
키 생성 지수	key generation exponent
키 생성 함수	key generating function
키 설정	key establishment
키 수송	key transport
키 요소	keying material
키 제어	key control
키 토큰	key token
키 확증	key confirmation
토큰	token
판결자	adjudicator
평문	plaintext
피드백 버퍼	feedback buffer
할당	assignment
할당 함수	assignment function
해쉬 코드	hash-code
해쉬 함수	hash-function
회신	response

3.2 영어 용어 중심의 가나다 순 나열

accreditation authority	인가 기관
accreditation multiplicity parameter	인가 증복 매개 변수
adjudicator	판결자
appendix	첨가
appendix function	첨가 함수
assignment	할당
assignment function	할당 함수
asymmetric cryptographic technique	비대칭 암호 기술
asymmetric encipherment system	비대칭 암호화 시스템
asymmetric key pair	비대칭 키 쌍
asymmetric signature system	비대칭 서명 시스템
bilateral counter	쌍방 계수기
block chaining	블록 연결

block	블록
certificate	인증서
certification authority(CA)	인증기관
challenge	접속
ciphertext, cipher text	암호문
collision-resistant hash-function	충돌 회피 해쉬 함수
commitment function	실행 함수
commitment	실행
cryptographic algorithm	암호 알고리즘
cryptographic check function	암호적 검사 함수
cryptographic check value	암호적 검사값
cryptographic synchronization	암호적 동기
data input	데이타 입력
data integrity	데이타 무결성
data object	데이타 객체
data storage	데이타 저장
data string(data)	데이타 문자열
decipherment	복호화
delivery authonity	전송 기관
digital signature	디지털 서명
distinguishing identifier	식별자
encipherment	암호화
entity authentication	실체 인증
evidence reqrester	증거 요청자
evidence	증거
exchange multiplicity parameter	교환 곱 매개 변수
feedback buffer	피드백 버퍼
half-block	반 블록
hash-code	해쉬 코드
hash-function	해쉬 함수
identity	정체성
implicit key authentication to A	객체 A에 대한 감추어진 키 인증
initializing value	초기 값
interleaving attack	인터리빙 공격
key agreement	키 동의
key confirmation	키 확증
key control	키 제어
key distribution centre(KDC)	키 분배 센터
key establishment	키 설정
key generating function	키 생성 함수
key generation exponent	키 생성 지수
keying material	키 요소
key material	키 관리
key token	키 토큰
key translation centre(KTC)	키 번역 센터
key transport	키 수송
key	키
masquerade	위장
message authentication code	메시지 인증 코드
messaage function	메시지 함수
message	메시지
modulus	법
n-bit block cipher algorithm	n-bit 블럭 암호 알고리즘

non-repudiation certificate
부인 봉쇄 인증서

non-repudiation exchange 부인 봉쇄 교환

non-repudiation information 부인 봉쇄 정보

non-repudiation of approval 승인 부인 봉쇄

non-repudiation of delivery 전송 부인 봉쇄

non-repudiation of knowledge
인지 부인 봉쇄

non-repudiation of origin 출처 부인 봉쇄

non-repudiation of receipt 수신 부인 봉쇄

non-repudiation of sending 송신 부인 봉쇄

non-repudiation of submission
제출 부인 봉쇄

non-repudiation of transport 운반 부인 봉쇄

non-repudiation policy 부인 봉쇄 정책

non-repudiation token 부인 봉쇄 토큰

NRD token NRD 토큰

NRO token NRO 토큰

NRS token NRS 토큰

NRT token NRS 토큰

one-way-function 일방향 함수

originating entity 근본 실체

originator 출처자

padding 덧붙이기

plaintext 평문

point-to-point key establishment
일대일 키 설정

pre-signature function 예비 서명 함수

pre-signature 예비 서명

private accreditation information
고유 인가 정보

private decipherment transformation
고유 복호화 함수

private key 고유 키

private signature exponent 고유 서명 지수

private signature key 고유 서명 키

proof 증명

public encipherment transfkormation
공개 암호화 함수

public key certificate 공개 키 인증서

public key function 공개 키 함수

public key information 공개 키 정보

public key 공개 키

public verification key 공개 증명 키

random number 난수

recipient 수신자

reduction function 감소 함수

redundancy 잉여 정보

redundant hash-function 잉여 해쉬 함수

redundant identity 잉여 정체성

reflection attack 반사 공격

replay attack 반복 공격

response 회신

round-function 라운드 함수

secret key 비밀 키

secret signature key 비밀 서명 키

secure envelope (SENV) 안전 봉투

security authority 보호 기관

security domain 보호 영역

signature equation 서명 방정식

signature key 서명 키

signature process	서명 과정
signature	서명
signed message	서명된 메시지
signer	서명자
starting variable (SV)	시작 변수
symmetric cryptographic technique	대칭 암호 기술
symmetric encipherment algorithm	대칭 암호화 알고리즘
symmetric technique	대칭 기술
system parameter	시스템 매개 변수
time stamp	시각 소인
time variant parameter	시간 변위 매개 변수
token	토큰
trusted third party	제 3의 신뢰 기관
unilateral authentication	일방 인증
verification exponent	증명 지수
verification function	증명 함수
verification key	증명 키
verification process	증명 과정
verifier	증명자
witness function	증거 함수
witness	증거
word	워드

참 고 문 헌

[Mi] WG2 Terminology Editor(C. J. Mitchell, U. K.), "SC27/WG2 Titles and Terminology (04/96), SC27 N1215

[한] 한국전자통신연구소, "OSI 한글용어 대비집", 1994

[청] 대한수학회, "수학용어집", 1995년, 청문각

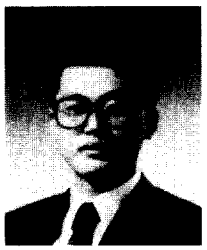
[교] 교육부, "교육부 편수자료집", 1994년, 교육부

[컴] 컴퓨터 용어 사전 편찬 위원회, "정보통신 용어 사전", 1996년, 크라운 출판사

□ 著者紹介

진 원 일

연세대학교 이과대학 수학과 졸업(이학사)
한국과학기술원 수학과 졸업(이학석사)
(주)한국마이크로소프트
연세대학교 본 대학원 수학과 박사과정

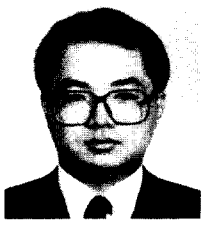


김 동 한

연세대학교 이과대학 수학과 졸업(이학사)
연세대학교 본 대학원 수학과 졸업(이학석사)
연세대학교 자연과학연구소

이 인 수

연세대학교 이과대학 수학과 졸업(이학사)
현재 연세대학교 본 대학원 수학과 석사과정



김 철

연세대학교 이과대학 수학과 졸업(이학사)
미국 North Carolina 주립대 대학원 수학과 졸업(이학석사.박사)
미국 North Carolina 주립대 수학과 시간강사
미국 Shaw University 전임강사
미국 University of South Dakota 수학과 부교수
현재 광운대학교 이과대학 수학과 부교수

※ 관심 분야 : 추상 대수학의 응용, 암호학의 수학적 이론 및 응용 등임.