공인인증서 발급을 위한 참조번호/인가코드 기술규격

The ReferenceValue/SecretValue Specification for Issuing Accredited Certificate

v1.11

2009년 9월

KISA 한국인터넷진흥원
Korea Internet & Security Agency

목 차

공인인증서 발급을 위한 참조번호/인가코드 기술규격

The ReferenceValue/SecretValue Specification
for Issuing Accredited Certificate

1. 목적

공인인증업무에 이용되는 참조번호/인가코드의 생성, 전달, 이용에 대한 규격을 정의한다.

2. 규격의 구성 및 범위

공인인증업무의 안전·신뢰성 제공을 위해 공인인증서 발급에 이용되는 참조번호/인가코드의 생성 규칙을 정의한다. 그리고, 생성 규칙에 의해 생성된 참조번호/인가코드를 가입자에게 전달하는 방법과 공인인증기관 또는 등록대행기관(이하 공인인증기관등)이 참조번호/인가코드 이용시 지켜야할 규칙을 정의한다.

3. 관련표준

3.1 국외 표준

[RFC2510] IETF RFC 2510(1999), Internet X.509 Public Key Infrastructure Certificate Management Protocols

3.2 국내 표준

[TTA-X.509] TTAS.IT-X509/R2(2000), 디렉토리 시스템 인증 프레임워크 표준
[KCAC.TS.CMP] KCAC.TS.CMP, v1.21, *공인인증서 관리 프로토콜 규격*, 2009

3.3 기타

해당사항 없음

4. 정의

4.1 전자서명법 정의

본 규격에서 사용된 다음의 용어들은 전자서명법 및 동법 시행령, 공인인증기관의 시설 및 장비 등에 관한 규정(미래창조과학부 고시)에 정의되어 있다.

가) 가입자
나) 공인인증업무
다) 공인인증기관
라) 공인인증서

4.2 공인인증서 발급을 위한 참조번호/인가코드 정의

본 규격의 목적을 위하여 다음과 같은 용어들을 정의한다.

가) 참조번호(Reference Value) : 공인인증서 발급시 메시지 출처인증을 위해 이용되는 값으로 인가코드를 식별하기 위해 사용됨([RFC2510] 참조)
나) 인가코드(Secret Value, Initial Authentication Key) : 공인인증서 발급시 메시지 출처인증을 위해 이용되는 값으로 인증서 관리 프로토콜 메시지의 메시지 인증 코드를 생성하기 위해 사용됨([RFC2510] 참조)

5. 약어

본 규격에서는 다음의 약어들이 이용된다.

가) CMP : Certificate Management Protocols, 인증서 관리 프로토콜
나) MAC : Message Authentication Code, 메시지 인증 코드

6. 참조번호/인가코드의 생성

이 장에서는 참조번호/인가코드를 생성하는 규칙을 정의한다.

6.1 참조번호

참조번호는 인가코드를 식별하기 위해 이용된다. 다음은 참조번호의 생성 규칙을 정의한 것이다.

- o Numeric, Alphanumeric 등을 이용할 수 있다.
- o 생성된 참조번호는 해당 인증시스템 내에서 오직 하나의 인가코드를 식별해야 한다.

6.2 인가코드

인가코드는 공인인증서 발급시 메시지 출처인증을 위해 이용되는 값으로 CMP 메시지의 MAC을 생성하기 위해 사용되며, 생성된 인가코드는 비밀정보로 이용되어야 한다. 다음은 인가코드의 생성 규칙을 정의한 것이다.

- o Numeric, Alphanumeric 등을 이용할 수 있다.
- o 인가코드는 랜덤하게 생성되어야 한다.
- o 인가코드의 최소길이

  - 3회 시도횟수 제한이 있을 경우

    ※ 3회 시도횟수 제한 : 가입자가 참조번호/인가코드를 3회 잘못 입력할 경우, 별도의 확인절차 없이 해당 공인인증서를 발급 받을 수 없음

Numeric	Alphanumeric[1)]
13	7

1) Alphanumeric : 대・소문자 구별됨

- 시도횟수 제한이 없을 경우

기간	Numeric	Alphanumeric[1)]
5일	13	7
10일	15	8
15일	17	9
20일	18	10
25일	20	11
30일	22	12

1) Alphanumeric : 대·소문자 구별됨

※ Numeric 또는 Alphanumeric을 이용하지 않을 경우에도 위의 보안성을 만족해야 함

7. 참조번호/인가코드의 전달

참조번호/인가코드는 해당 공인인증기관등과 가입자의 직접대면을 통해 전달되는 것을 원칙으로 한다. 직접대면 전달을 통해 제공되는 보안성은 다음과 같다.

o 참조번호/인가코드가 해당 가입자에게 전달됨이 보장되어야 한다.
o 참조번호/인가코드 전달시 기밀성이 제공되어야 한다.

공인인증기관등이 직접대면이 아닌 다른 방법으로 참조번호/인가코드를 가입자에게 전달할 경우에도 직접대면을 이용해 참조번호/인가코드를 전달하는 방법이 가지는 보안성을 유지해야 한다.

8. 참조번호/인가코드의 이용

다음은 참조번호/인가코드를 이용해 공인인증서를 발급할 경우 공인인증기관등이 준수해야할 규칙을 정의한 것이다.

o 공인인증서 발급을 위해 생성 및 전달된 참조번호/인가코드는 오직 한번의 공인인증서 발급을 위해서만 이용되어야 하며, 같은 참조번호/인가코드가

다른 공인인증서 발급을 위해 재사용 되어서는 안 된다.

- o 전달받은 참조번호/인가코드를 이용해 해당 공인인증서를 발급 받을 수 있는 기한은 인가코드의 최소길이에 준한다.(6.2 참조) 단, 3회 시도횟수 제한이 있을 경우에는 30일 이내로 한정한다.

9. 부가적 정보의 이용

공인인증기관등이 공인인증서 발급에 이용되는 참조번호/인가코드를 가입자에게 전달하기 위해 부가적 정보들(예 : ID, Password, 일회성 정보 등)을 이용할 수 있다.

부록 1. 규격 연혁

버전	제・개정일	제・개정내역
v1.00	2003년 5월	・"공인인증서 발급을 위한 참조번호/인가코드 기술규격"으로 제정
v1.10	2008년 10월	・관련 국내 표준 및 규격 갱신 내용 반영 ・법률 공포번호가 해당 법률 개정시마다 변경되는 점을 고려하여 법령명으로 개정
v1.11	2009년 9월	・공인전자서명인증체계 기술규격 개정에 따라 본문 내용 중 관련 기술규격 참조 변경 사항 개정