공인인증서를 이용한 본인확인 서비스 가이드라인

Accredited Certificate-based Identification Service Guideline

v1.0

2012년 11월

KISA 한국인터넷진흥원
Korea Internet & Security Agency

목 차

공인인증서를 이용한 본인확인 서비스 가이드라인
Accredited Certificate-based Identification Service Guideline

1. 개 요

본 안내서는 인터넷 상에서 개인정보 없이 회원가입, 로그인이 가능하도록 공인인증서를 이용하는 경우에 사용자, 인터넷 서비스 제공자, 공인인증기관간의 통신에서 해당 정보의 노출 없이 안전하게 관련정보를 생성, 전달 그리고 검증하기 위한 절차를 명시한다.

2. 가이드라인의 구성 및 범위

본 가이드라인에서는 인터넷 상에서 개인정보 보호수단으로 공인인증서를 이용하는데 필요한 문법 및 절차를 크게 3부분으로 나누어 기술한다.

첫 번째로, 공인전자서명인증체계에서 공통적으로 이용되는 공인인증서를 이용한 본인확인(UCPID) 서비스의 구성 및 운영과 개인식별정보를 요청 및 검증하는 전체적인 절차에 대해 기술하고 있다.

두 번째로, 공인인증서를 이용한 본인확인(UCPID) 서비스에서 구체적으로 정의되어야 할 UCPID 요청·응답 메시지 형식을 ASN.1 구문으로 기술하고 있다.

세 번째로, UCPID 요청·응답 메시지의 본인인증, 무결성 및 기밀성을 제공하기 위한 전자서명과 암호화방식에 대해 기술하고 있다.

3. 관련 표준

3.1 국외 표준 및 규격

[X509]	ITU-T Recommendation X.509 (2000) | ISO/IEC 9594-8:2000, Information technology - Open Systems Interconnection - The Directory: Authentication Framework
[X609]	ITU-T Recommendation X.609 (2002) | ISO/IEC 8825-1:2002, Information technology - ASN.1

Encoding Rules : Specification Of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) And Distinguished Encoding Rules (DER)

[RFC2119] IETF, RFC2119, Key words for use in RFCs to Indicate Requirement Levels, March 1997

[RFC3280] IETF RFC 3280, Internet X.509 Public Key Infrastructure: Certificate and CRL Profile, 2002

[PKCS7] RSA Laboratories PKCS#7 v1.5, Cryptographic Message Syntax Standard, 1993

[RFC3275] IETF, RFC3275, (Extensible Markup Language) XML-Signature Syntax and Processing, March 2002

[RFC2119] IETF, RFC2119, Key words for use in RFCs to Indicated Requirement Levels, March 1997

[RFC2279] IETF, RFC2279, UTF-8, a transformation format of ISO 10646, January 1998

[XMLDSIG] XML, XML-Signature Syntax and Processing, February, 2002

[XMLENC] XML, XML Encryption Syntax and Processing, December, 2002

3.2 국내 표준 및 규격

[KCAC.TS.DSIG] KISA, KCAC.TS.DSIG v1.30, 전자서명 알고리즘 규격, 2009

[KCAC.TS.ENC] KISA, KCAC.TS.ENC v1.21, 암호 알고리즘 규격, 2009

3.3 기타

해당사항 없음

4. 정의

4.1 전자서명법 용어 정의

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

가) 전자서명키, 전자서명생성키, 전자서명검증키
나) 공인인증서
다) 공인인증기관
라) 전자서명인증관리체계
마) 가입자
바) 이용자

4.2 용어의 정의

본 가이드라인을 위하여 다음과 같은 용어들을 정의한다.

가) 주민등록번호 : 「주민등록법」 제7조제3항에 따라 시장·군수 또는 구청장이 부여한 개인별로 고유한 등록번호

나) i-PIN(본인확인정보) : 본인확인을 수행한 이후 본인확인기관이 이용자에게 부여하는 식별정보

다) i-PIN 서비스 : 인터넷상에서 i-PIN(본인확인정보)을 이용하여 이용자를 안전하게 식별·인증하기 위해 본인확인기관이 제공하는 서비스

라) 본인확인기관 : i-PIN서비스를 이용자 및 인터넷 서비스 제공자에 제공하는 자

마) 인터넷 서비스 제공자(ISP) : 업무상 인터넷을 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자

바) 인터넷 웹사이트 : 인터넷 서비스 제공자가 운영하는 웹사이트

사) 개인정보 : 생존하는 개인에 관한 정보로서 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함)로써, 본 가이드라인에서는 인증서고유명, 인증서 상태값, 중복가입확인정보, 연계정보, 생년월일, 성별, 내·외국인정보 등을 의미

아) 식별번호 : 「전자서명법 시행규칙」 제13조의2에 의한 주민등록번호, 사업자등록번호 및 고유번호

자) 웹사이트 식별번호 : 인터넷 서비스 제공자가 운영하는 웹사이트를 다른 웹사이트와 구별하기 위하여 본인확인기관이 부여한 정보

차) 중복가입확인정보(DI) : 인터넷사업자가 운영하는 웹사이트에 가입하

고자 하는 이용자의 중복가입 여부를 확인하는데 사용되는 정보로서 본인확인기관이 이용자의 주민등록번호, 웹사이트 식별번호 및 본인확인기관간 공유비밀번호를 이용하여 생성한 정보

카) 연계정보(CI) : 서비스 연계를 위해 본인확인기관에서 부여하는 개인식별정보

타) 개인식별정보 : 개인식별을 위하여 공인인증기관이 가입자에게 부여하는 식별정보로 본인확인기관에서 부여하는 중복가입확인정보(DI)와 연계정보(CI)

파) 연계 공인인증기관 : ISP와 UCPID서비스 제공 계약을 맺은 공인인증기관

하) 발급 공인인증기관 : 이용자 공인인증서를 발급한 공인인증기관

4.3 용어의 효력

본 가이드라인에서 사용된 다음의 용어들은 공인인증기관 및 가입자 소프트웨어가 공인인증서를 이용한 본인확인(UCPID) 서비스를 제공하거나 처리하는데 따라야 할 구현 정도를 의미하는 것으로 [RFC2119]를 준용하며 다음과 같은 의미를 지닌다.

가) 해야 한다, 필수이다, 강제한다. (기호 : M)
반드시 준수해야 한다.

나) 권고한다. (기호 : R)
보안성 및 상호연동을 고려하여 준수할 것을 권장한다.

다) 할 수 있다, 쓸 수 있다. (기호 : O)
주어진 상황을 고려하여 필요한 경우에 한해 선택적으로 사용할 수 있다.

라) 권고하지 않는다. (기호 : NR)
보안성 및 상호연동을 고려하여 사용하지 말 것을 권장한다.

마) 금지한다, 허용하지 않는다. (기호 : X)
반드시 사용하지 않아야 한다.

바) 언급하지 않는다, 정의하지 않는다. (기호 : -)
준수 여부에 대해 기술하지 않는다.

5. 약어

본 규격에서는 다음의 약어가 이용된다.

가) RN : Resident Number, 주민등록번호(이하 주민번호)
나) CI : Connection Information, 연계 정보
다) DI : Duplication Information, 중복가입확인정보
라) UCPID : Use of accredited Certificate for Personal IDentification, 공인인증서를 이용한 본인확인
마) ISP : Internet Service Provider, 인터넷 서비스 제공자

6. 공인인증서를 이용한 본인확인(UCPID) 서비스 모델

6.1 UCPID 서버 구성 및 운영

공인인증기관이 공인인증서를 이용한 본인확인(UCPID) 서비스를 제공하고자 하는 경우 공인인증서를 발급하는 인증서 생성·관리 설비와는 다른 장비에서 UCPID 서버를 운영해야 한다.

UCPID 서버는 가입자의 공인인증서를 이용한 개인식별정보 생성 및 검증 요청에 응답하기 위한 공인인증서 상태 확인을 위해 항상 최신의 공인인증서 효력정지 및 폐지목록 정보를 인증서 생성·관리 시스템 또는 디렉토리 서버로부터 획득해야 한다. 만일 공인인증서 효력정지 및 폐지목록 정보 획득을 위해 UCPID 서버와 인증서 생성·관리 시스템이 연결될 경우에는 상호간에 접근통제 기능과 데이터의 무결성이 반드시 보장되어야 한다.

또한, UCPID 서버의 전자서명키는 공인인증서비스의 안전·신뢰성 측면에서 인증서 생성·관리 설비의 전자서명키와 동일해서는 안된다.

6.2. UCPID 이용절차

공인인증서를 이용한 본인확인(UCPID) 서비스는 공인전자서명인증체계에서 공인인증서를 이용하여 본인확인과 ISP가 필요로 하는 개인정보를 제공하는 서비스로 인터넷 상에서 개인정보보호 수단으로 회원가입, 로그인, ID·패스워드 찾기 등 본인확인이 필요한 서비스에 사용된다.

UCPID 이용절차는 [그림1]과 같다. 이용자는 회원가입, 로그인 등을 위하여

ISP에 접속한다. ISP는 이용자에게 인증서 및 개인정보활용(수집, 제공, 활용, 관리

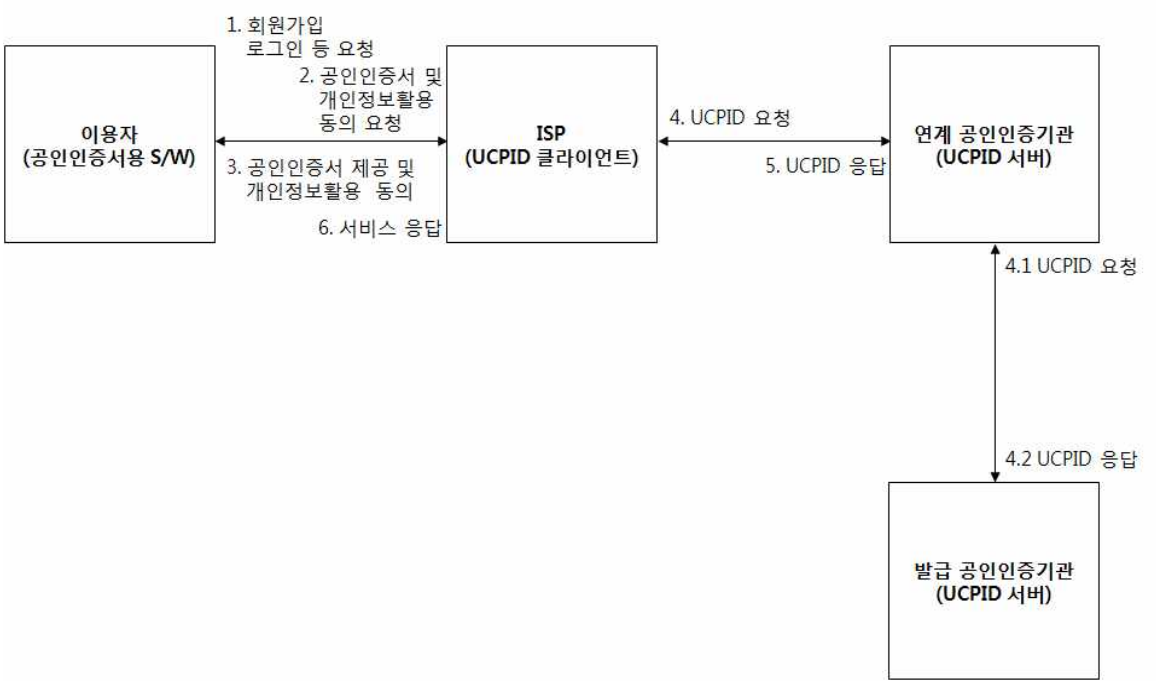

그림 1 UCPID 이용절차

등) 동의약관을 포함하는 웹 페이지를 제공한다. 이용자는 개인정보활용 동의 약관과 동의여부에 전자서명하고 공인인증서와 함께 ISP에 제공한다.

ISP는 이용자의 개인정보활용 동의 메시지와 공인인증서 그리고 ISP 구분정보, 필요 개인정보항목과 키분배용 인증서 등을 포함하는 UCPID 요청메시지를 생성하여 공인인증기관에게 제공한다. UCPID 요청 메시지는 전송 채널 보안 혹은 전자서명 등, 메시지의 무결성을 보장할 수 있는 방안을 마련하여 전달해야 한다.

공인인증기관은 제공된 공인인증서의 유효성을 검증하고, 유효성 검증 결과와 개인식별정보 그리고 요청된 개인정보를 포함하는 UCPID 응답메시지를 생성하여 ISP로 전달한다. UCPID 응답메시지는 전자서명 후 암호화하여 전달한다.

단, 이용자 공인인증서의 발급 공인인증기관이 연계 공인인증기관과 동일하지 않을 경우, 연계 공인인증기관은 UCPID 요청메시지를 연계 공인인증기관 전자서명용 인증서 및 개인키로 전자서명하여 발급 공인인증기관으로 전달한다.

발급 공인인증기관은 UCPID 응답메시지를 생성하여 연계 공인인증기관으로 전달한다. 발급 공인인증기관은 ISP에 제공할 개인정보를 ISP의 키분배용 인증서로 반드시 암호화하여 UCPID 응답메시지를 생성 및 전자서명 하여 연계 공인인증기관으로 전달한다. 연계 공인인증기관은 UCPID 응답메시지를 ISP로 전달한다.

6.3 UCPID 공인인증서

UCPID 서버용 공인인증서 프로파일은 [KCAC.TS.DSCP]을 준용하여 공인인증기관이 자체적으로 발급할 수 있다. 공인인증기관이 자체적으로 발급하는 경우 반드시 최상위인증기관으로부터 발급받은 공인인증기관의 공인인증서에 포함된 전자서명키를 사용해야 한다.

7. UCPID 메시지 규격

7.1 구성 및 범위

공인인증서를 이용한 본인확인(UCPID) 서비스에서 사용되는 메시지들을 도출하고 각 메시지에 대한 표준을 정의한다. 서비스에서 사용되는 메시지들은 [그림2]와 같이 각각의 생성주체에 의해 생성되고, 전자서명/암호화되어 전달된다.

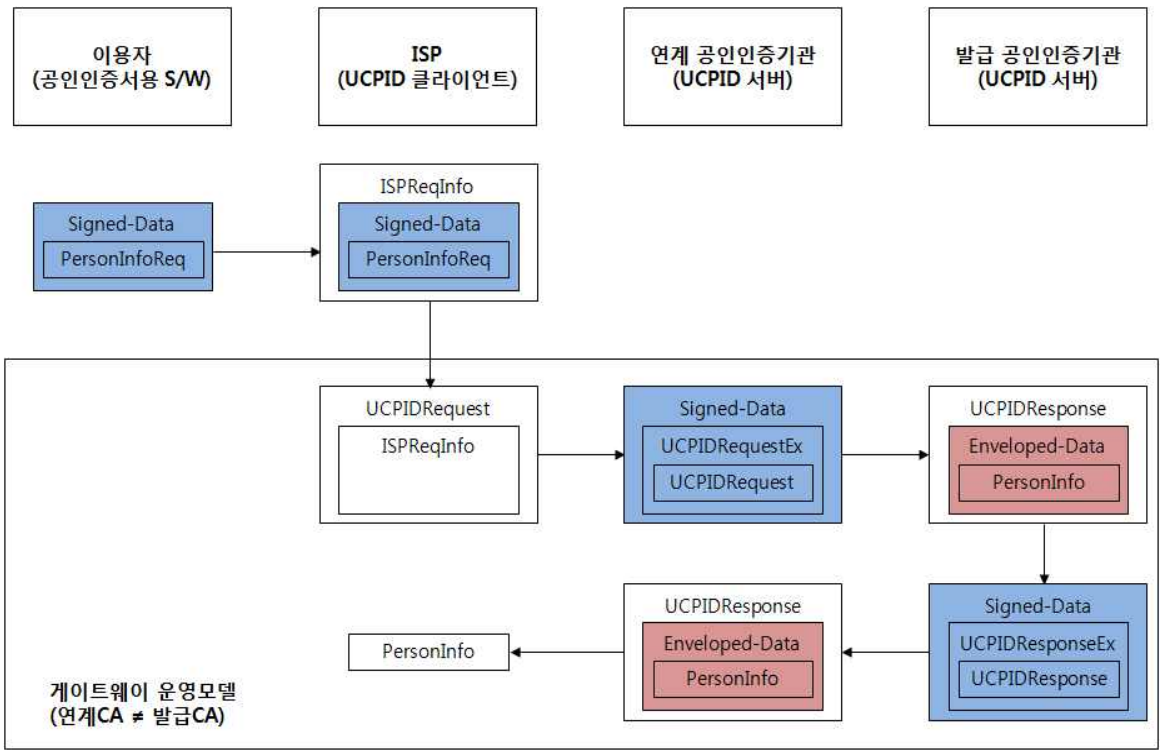

그림 2 UCPID 메시지 규격

7.2 PersonInfoReq

개인정보활용 동의 요청(PersonInfoReq) 메시지는 개인정보활용 동의 약관과 동의 여부로 구성해야 한다.

```
PersonInfoReq   ::= SEQUENCE {
        userAgreement           UTF8String,
         -- 개인정보제공 및 활용동의 약관
        userAgree               userAgreeInfo
         -- ISP에서 필요로 하는 개인정보 항목 중 사용자 동의 항목
}
userAgreeInfo ::== BIT STRING {
        realName                (0),
        gender                  (1),
        nationalInfo            (2),
        birthDate               (3)
        -- ISP에서 필요로 하는 개인정보 항목 중 사용자 동의 항목
}
```

7.3 UCPIDRequest

UCPID 요청 메시지(UCPIDRequest)는 발급 공인인증기관 식별정보와 ISP 요청 정보(ISPReqInfo)로 구성된다.

UCPIDRequest의 ASN.1 표현 형식은 다음과 같다.

```
UCPIDRequest    ::= SEQUENCE {
        issuerKeyHash           OCTET STRING,
         -- 발급 공인인증기관 식별정보로 공인인증기관 공개키 해쉬값
        cpCode                  PrintableString,
        -- 연계 공인인증기관이 ISP에 부여하는 코드(12자리)
        contentISPReqInfo       UCPIDContentInfo
         -- contentISPReqInfo는 ISPReqInfo의 평문(PKCS#7 data Type)
         -- 또는, ISPReqInfo의 전자서명된 형태 (PKCS#7 SignedData Type)
}

UCPIDContentInfo ::= ContentInfo
  -- CotentType은 [PKCS#7]에 정의된 id-data, id-signedData 중 하나이다.
```

contentISPReqInfo는 ISPReqInfo의 평문형태 또는 전자서명된 형태로 생성해야 한다.

contentISPReqInfo는 전송 프로토콜에서 무결성 보장 방안이 있는 경우 ISPReqInfo의 평문형태로 생성하고, 그렇지 않을 경우 ISPReqInfo의 전자서명 형태로 생성 하여야 한다.

연계 공인인증기관에서 발급 인증기관으로 전송 시, 공인인증기관간 UCPID요청 메시지(UCPIDRequestEx)를 생성하고, 이를 전자서명하여 제공한다.

7.3.1 ISPReqInfo

ISP요청정보는 ISP 식별정보, ISP 필요 개인정보, ISP 세션정보, 비표(Nonce), ISP 키분배용 인증서, 전자서명된 개인정보제공 및 활용 동의 요청(PersonInfoReq)을 포함한다.

ISPReqInfo의 ASN.1 표현 형식은 다음과 같다.

```
ISPReqInfo      ::= SEQUENCE {
        version                 UCPIDVersion,
        -- 버전
        ucpidNonce              UCPIDNonce,
        -- 비표(Nonce)는 UCPID 요청 및 응답을 재연공격(replay attack)으로
        -- 부터 안전하게 전송하기 위해 활용
        cpRequestNumber         PrintableString,
        -- ISP가 부여하는 세션정보로 이용자 개인정보를 ISP가 공인인증기관
        -- 으로부터 제공받기 위해 활용
        ispKmCert               CertificateInfo,
        -- ISP의 키분배용 인증서로 연계/발급 인증기관에서 ISP로 개인정보
        -- 를 안전하게 암호화하여 전송 시 활용
        signedPersonInfoReq     UCPIDContentInfo
        -- 개인정보제공 및 활용 동의 요청(PersonInfoReq)에 이용자
        -- 전자서명 개인키로 전자서명한 값(PKCS#7 signedData Type)
}

UCPIDVersion ::= INTEGER { v1(1) }

UCPIDNonce ::== OCTET STRING

CertificateInfo ::= Certificate
```

7.3.2 UCPIDRequestEx

연계 공인인증기관에서 발급 공인인증기관으로 보내는 요청메시지는 UCPID 요청 메시지(UCPIDRequest), 비표(Nonce), 공인인증기관 세션정보, 연계 공인인증기관 식별정보를 포함하고 전자서명하여 제공된다.

```
UCPIDRequestEx  ::= SEQUENCE {
        version                 UCPIDVersion,
        -- 버전
        ucpidNonce              UCPIDNonce,
        -- 비표(Nonce)는 공인인증기관 간 UCPID 요청 및 응답을 재연공격
        -- (replay attack)으로부터 안전하게 전송하기 위해 활용
        caKeyHash               OCTET STRING,
        -- 연계 공인인증기관 식별정보로 공인인증기관 공개키 해쉬값
        caRequestNumber         PrintableString,
        -- 연계 공인인증기관이 부여하는 세션정보로 이용자의 개인정보를
        -- 연계 공인인증기관이 발급 공인인증기관으로부터 제공받기 위해
        -- 활용
        contentUCPIDRequest     UCPIDRequest
        -- 연계 공인인증기관에서 생성한 UCPID 요청메시지
        -- UCPIDRequest 내 contentISPReqInfo 는 data type 으로 처리
}
```

7.4 UCPIDResponse

UCPID 응답 메시지(UCPIDResponse)는 발급 공인인증기관 식별정보와 암호화된 개인정보(PersonInfo)로 구성된다.

UCPIDResponse의 ASN.1 표현 형식은 다음과 같다.

```
UCPIDResponse   ::= SEQUENCE {
        issuerKeyHash           OCTET STRING,
         -- 발급 공인인증기관 식별정보로 공인인증기관 공개키 해쉬값
        status                  UCPIDStatus,
        -- 요청/응답 메시지의 상태
        contentPersonInfo       UCPIDContentInfo        OPTIONAL
         -- contentPersonInfo는 PersonInfo의 평문(PKCS#7 data Type)
         -- 또는 PersonInfo의 암호문(PKCS#7 envelopedData Type)
         -- 암호화의 원문은 PersonInfo의 전자서명된 형태
```

```
        -- (PKCS#7 signedData Type)
}

UCPIDStatus             ::= SEQUENCE {
        statusCode              UCPIDStatusCode,
        statusString            PKIFreeText     OPTIONAL
}

UCPIDStatusCode ::= BIT STRING {
        okay                    (0),
        badRequest              (1),
        tooBusy                 (2),
        undefined               (3),
        badStructure            (20),
        unsupportedVersion      (21),
        unableToDecode          (22),
        badSignature            (30),
        notAuthorized           (31),
        unsupportedSignature    (32),
        invalidSignature        (33),
        systemFailure           (40),
        invalidCertificate      (41)
}
```

contentPersonInfo는 UCPIDStatusCode의 값이 'okay'인 경우 반드시 포함되어야 하며, 그 이외의 값인 경우 contentPersonInfo를 생성하지 않는다.

contentPersonInfo는 PersonInfo의 평문형태 또는 암호화된 형태로 생성 하여야 한다. 암호화된 형태로 생성하는 경우 발급 공인인증기관의 전자서명생성키로 전자서명 후 암호화해야 한다. 암호화에 필요한 키분배용 인증서는 ISPReqInfo에 포함된 ispkmCert를 활용한다.

contentPersonInfo는 전송 프로토콜에서 전자서명 암호화가 이루어질 경우 PersonInfo의 평문형태로 생성하고, 그렇지 않을 경우 PersonInfo의 암호화된 형태로 생성 하여야 한다. 단, 이용자 공인인증서의 발급 공인인증기관이 연계 공인인증기관과 동일하지 않을 경우, contentPersonInfo는 공인인증기관간 호환성 확보를 위해 암호화된 형태로 생성하여야 한다. 암호화된 형태로 생성 시 [PKCS7] 규격을 준용하여 전자서명 후 암호화 하여야 한다.

7.4.1 PersonInfo

개인정보 응답정보(PersonInfo)는 이용자 공인인증서의 고유명, 공인인증서 상태, ISP식별정보, 연계정보, 중복가입 확인정보와 ISP에서 요청한 개인정보를 포함한다.

```
PersonInfo      ::= SEQUENCE {
        version                 UCPIDVersion,
        -- 버전
        ucpidNonce              UCPIDNonce,
        -- 비표(Nonce)는 UCPID 요청 및 응답을 재연공격(replay attack)으로
        -- 부터 안전하게 전송하기 위해 활용되는 값으로 ISPReqInfo의
        -- ucpidNonce값과 동일
        cpRequestNumber         PrintableString,
        -- ISP가 부여하는 세션정보로 이용자 개인정보를 ISP가 공인인증기관
        -- 으로부터 제공받기 위해 활용
        certDn                  Name,
        -- 이용자 공인인증서 고유명
        cpCode                  PrintableString,
        -- 연계 공인인증기관이 ISP에 부여하는 코드(12자리)
        ci                      PrintableString,
        -- 이용자의 연계정보(PEM)
        di                      [0]     PrintableString,
        -- 이용자의 중복가입 확인정보(PEM)
        realName                [1]     UTF8String OPTIONAL,
        -- 이용자의 실명
        gender                  [2]     PersonInfoGender OPTIONAL,
        -- 이용자의 성별 { 여성(0), 남성(1) }
        nationalInfo            [3]     PersonInfoNationalInfo OPTIONAL,
        -- 내외국인 정보 { 내국인(0), 외국인(1) }
        birthDate               [4]     NumericString OPTIONAL
}

PersonInfoGender ::= ENUMERATED {
        female                  (0),    -- 여자
        male                    (1)     -- 남자
}

PersonInfoNationalInfo ::= ENUMERATED {
        resident                (0),    -- 내국인
```

```
        foreigner               (1)     -- 외국인
}
```

7.4.2 UCPIDResponseEx

발급 공인인증기관에서 연계 공인인증기관으로 보내는 요청메시지는 UCIPID 응답메시지(UCPIDResponse), 비표(Nonce), 공인인증기관 세션정보, 연계 공인인증기관 식별정보를 포함하고, 전자서명하여 제공된다.

```
UCPIDResponseEx ::= SEQUENCE {
        version                 UCPIDVersion,
        -- 버전
        status                  UCPIDStatus,
        -- 요청/응답 메시지의 상태
        ucpidNonce              UCPIDNonce,
        -- 비표(Nonce)는 공인인증기관간 UCPID 요청 및 응답을 재연공격
        -- (replay attack)으로부터 안전하게 전송하기 위해 활용되는 값으로
        -- UCPIDRequestEx의 ucpidNonce값과 동일
        caKeyHash               OCTET STRING,
        -- 연계 공인인증기관 식별정보로 공인인증기관 공개키 해쉬값
        caRequestNumber         PrintableString,
        -- 연계공인인증기관이 부여하는 세션정보로 이용자의 개인정보를
        -- 연계공인인증기관이 발급 공인인증기관으로부터 제공받기 위해
        -- 활용
        contentUCPIDResponse    UCPIDResponse
        -- 발급 인증기관에서 생성한 UCPID 응답메시지
}
```

8. 프로토콜 규격

8.1 개요

공인인증서 이용기술 서비스의 활성화를 위해서는 서로 다른 서비스 주체들의 시스템 간 통신이 가능하여야 하며, 이를 위해서는 표준화된 메시지 규격이 필수적이다. 본 가이드라인에서는 이러한 메시지 규격에 대해서 기술한다.

8.2 구성 및 범위

본 가이드라인에서는 각 서비스 시스템 간의 통신을 위한 메시지 규격을 설명한다. 메시지 전송 시에 사용하는 프로토콜과 전송 메시지의 형식, 그리고 시스템 간에 이루어지는 메시지들에 대해 설명한다.

본 가이드라인에서는 상호연동을 위해 필요한 시스템 간에 이루어지는 메시지에 대해서만 기술하며 그 밖의 시스템 내부 메시지에 대해서는 규정하지 않는다.

8.3 전송 프로토콜

공인인증서 이용기술 서비스에서 사용되는 전송 프로토콜은 아래와 같은 기본적인 요구사항을 만족해야 한다.

- 국제표준 프로토콜을 사용하여 글로벌 인프라와의 연동이 가능해야 한다.
- 인터넷 기반에서 범용적으로 사용되는 프로토콜을 수용해야 한다.
- 기능에 있어서 확장이 가능한 형태이어야 한다.

본 메시지 규격은 상기의 모든 요구사항을 수용할 수 있는 인터넷 관련 표준 프로토콜 규격을 준수하도록 한다.

8.4 보안 프로토콜

인터넷에서의 대표적인 보안 프로토콜은 아래와 같이 정의할 수 있다.

- 네트워크(IP) 레벨 : IPSec
- 트랜스포트(TCP) 레벨 : SSL/TLS
- 애플리케이션 레벨 : SSH, Kerberos 등

이러한 구분을 바탕으로 보안 프로토콜을 적용함에 있어서, 공인인증서 이용 기술 프로토콜 표준에서는 애플리케이션 레벨의 보안, 즉 메시지 보안을 위하여, 다음과 같은 표준 규격을 사용하도록 한다.

- ISP와 공인인증기관 구간 : PKCS#7 혹은 XML Signature
- 연계 공인인증기관과 발급 공인인증기관 구간 : PKCS#7

PKCS#7 규격을 이용한 메시지를 이용하는 경우, PKCS#7 메시지 앞에 메시지 길이를 의미하는 4바이트 메시지를 추가한다.

본 가이드라인에서 사용하는 XML 전자서명은 [RFC3275], [XMLDSIG]를 사용하며, XML 암호화는 [XMLENC]를 사용한다.

통신채널 보안을 위해 ISP와 공인인증기관간에 선택적으로 SSL/TLS를 사용할 수 있다.

8.4.1 PKCS#7 을 이용한 암호화 및 전자서명

소켓(TCP/IP)을 이용한 메시지 전달방법에서는 [PKCS7]의 Signed-data content type 및 Enveloped-data content type 규격을 준용한다.

부록 1. ASN.1 표현 형식

```
DEFINITIONS EXPLICIT TAGS ::=

BEGIN

-- EXPORTS All
-- The types and values defined in this module are exported for use
-- in the other ASN.1 modules.  Other applications may use them for
-- their own purposes.

IMPORTS

    Certificate, CertificateSerialNumber, Name, CRLReason, Extensions
         FROM PKIX1Explicit88
             { iso(1) identified-organization(3) dod(6)
               internet(1) security(5) mechanisms(5) pkix(7)
               mod(0) pkix1-explicit(18) }

    ContentInfo
         FROM PKCS#7

    PKIFreeText
         FROM PKIXCMP

PersonInfoReq   ::= SEQUENCE {
        userAgreement           UTF8String,
         -- 개인정보제공 및 활용동의 약관
        userAgree               userAgreeInfo
         -- ISP에서 필요로 하는 개인정보 항목 중 사용자 동의 항목
}
userAgreeInfo ::== BIT STRING {
      realName                  (0),
      gender                    (1),
      nationalInfo              (2),
      birthDate                 (3)
      -- ISP에서 필요로 하는 개인정보 항목 중 사용자 동의 항목
}

UCPIDRequest    ::= SEQUENCE {
        issuerKeyHash           OCTET STRING,
         -- 발급 공인인증기관 식별정보로 공인인증기관 공개키 해쉬값
        cpCode                  PrintableString,
        -- 연계 공인인증기관이 ISP에 부여하는 코드(12자리)
```

```
        contentISPReqInfo       UCPIDContentInfo
         -- contentISPReqInfo는 ISPReqInfo의 평문(PKCS#7 data Type)
         -- 또는, ISPReqInfo의 전자서명된 형태 (PKCS#7 SignedData Type)
}

UCPIDContentInfo ::= ContentInfo
  -- CotentType은 [PKCS#7]에 정의된 id-data, id-signedData 중 하나이다.

ISPReqInfo      ::= SEQUENCE {
        version                 UCPIDVersion,
        -- 버전
        ucpidNonce              UCPIDNonce,
        -- 비표(Nonce)는 UCPID 요청 및 응답을 재연공격(replay attack)으로
        -- 부터 안전하게 전송하기 위해 활용
        cpRequestNumber         PrintableString,
        -- ISP가 부여하는 세션정보로 이용자 개인정보를 ISP가 공인인증기관
        -- 으로부터 제공받기 위해 활용
        ispKmCert               CertificateInfo,
        -- ISP의 키분배용 인증서로 연계/발급 인증기관에서 ISP로 개인정보
        -- 를 안전하게 암호화하여 전송 시 활용
        signedPersonInfoReq     UCPIDContentInfo
        -- 개인정보제공 및 활용 동의 요청(PersonInfoReq)에 이용자
        -- 전자서명 개인키로 전자서명한 값(PKCS#7 signedData Type)
}

UCPIDNonce ::== OCTET STRING

UCPIDVersion ::= INTEGER { v1(1) }

CertificateInfo ::= Certificate

UCPIDRequestEx  ::= SEQUENCE {
        version                 UCPIDVersion,
        -- 버전
        ucpidNonce              UCPIDNonce,
        -- 비표(Nonce)는 공인인증기관 간 UCPID 요청 및 응답을 재연공격
        -- (replay attack)으로부터 안전하게 전송하기 위해 활용
        caKeyHash               OCTET STRING,
        -- 연계 공인인증기관 식별정보로 공인인증기관 공개키 해쉬값
        caRequestNumber         PrintableString,
```

```
        -- 연계 공인인증기관이 부여하는 세션정보로 이용자의 개인정보를
        -- 연계 공인인증기관이 발급 공인인증기관으로부터 제공받기 위해
        -- 활용
        contentUCPIDRequest    UCPIDRequest
        -- 연계 공인인증기관에서 생성한 UCPID 요청메시지
        -- UCPIDRequest 내 contentISPReqInfo 는 data type 으로 처리
}

UCPIDResponse   ::= SEQUENCE {
        issuerKeyHash           OCTET STRING,
         -- 발급 공인인증기관 식별정보로 공인인증기관 공개키 해쉬값
        status                  UCPIDStatus,
        -- 요청/응답 메시지의 상태
        contentPersonInfo       ContentInfo OPTIONAL
         -- contentPersonInfo는 PersonInfo의 평문(PKCS#7 data Type)
         -- 또는 PersonInfo의 암호문(PKCS#7 envelopedData Type)
         -- 암호화의 원문은 PersonInfo의 전자서명된 형태
         -- (PKCS#7 signedData Type)
}

UCPIDStatus             ::= SEQUENCE {
        statusCode              UCPIDStatusCode,
        statusString            PKIFreeText             OPTIONAL
}

UCPIDStatusCode ::= BIT STRING {
        okay                    (0),
        badRequest              (1),
        tooBusy                 (2),
        undefined               (3),
        badStructure            (20),
        unsupportedVersion      (21),
        unableToDecode          (22),
        badSignature            (30),
        notAuthorized           (31),
        unsupportedSignature    (32),
        invalidSignature        (33),
        systemFailure           (40),
        invalidCertificate      (41)
}
```

```
PersonInfo      ::= SEQUENCE {
        version                 UCPIDVersion,
        -- 버전
        ucpidNonce              UCPIDNonce,
        -- 비표(Nonce)는 UCPID 요청 및 응답을 재연공격(replay attack)으로
        -- 부터 안전하게 전송하기 위해 활용되는 값으로 ISPReqInfo의
        -- ucpidNonce값과 동일
        cpRequestNumber         PrintableString,
        -- ISP가 부여하는 세션정보로 이용자 개인정보를 ISP가 공인인증기관
        -- 으로부터 제공받기 위해 활용
        certDn                  Name,
        -- 이용자 공인인증서 고유명
        cpCode                  PrintableString,
        -- 연계 공인인증기관이 ISP에 부여하는 코드(12자리)
        ci                      PrintableString,
        -- 이용자의 연계정보(PEM)
        di                      PrintableString,
        -- 이용자의 중복가입 확인정보(PEM)
        realName                [0]     UTF8String OPTIONAL,
        -- 이용자의 실명
        gender                  [1]     PersonInfoGender OPTIONAL,
        -- 이용자의 성별 { 여성(0), 남성(1) }
        nationalInfo            [2]     PersonInfoNationalInfo OPTIONAL,
        -- 내외국인 정보 { 내국인(0), 외국인(1) }
        birthDate               [3]     NumericString OPTIONAL,
        -- YYYYMMDD 8자리 숫자의 이용자 생년월일 정보
}

PersonInfoGender ::= ENUMERATED {
        female                  (0),    -- 여자
        male                    (1)     -- 남자
}

PersonInfoNationalInfo ::= ENUMERATED {
        resident                (0),    -- 내국인
        foreigner               (1)     -- 외국인
}

UCPIDResponseEx ::= SEQUENCE {
```

```
        version                 UCPIDVersion,
        -- 버전
        status                  UCPIDStatus,
        -- 요청/응답 메시지의 상태
        ucpidNonce              UCPIDNonce,
        -- 비표(Nonce)는 공인인증기관 간 UCPID 요청 및 응답을 재연공격
        -- (replay attack)으로부터 안전하게 전송하기 위해 활용되는 값으로
        -- UCPIDRequestEx의 ucpidNonce값과 동일
        caKeyHash               OCTET STRING,
        -- 연계 공인인증기관 식별정보로 공인인증기관 공개키 해쉬값
        caRequestNumber         PrintableString,
        -- 연계공인인증기관이 부여하는 세션정보로 이용자의 개인정보를
        -- 연계공인인증기관이 발급 공인인증기관으로부터 제공받기 위해
        -- 활용
        contentUCPIDResponse    UCPIDResponse
        -- 발급 인증기관에서 생성한 UCPID 응답메시지
}

END - of UCPID
```

부록 2. 가이드라인 연혁

버전	제.개정일	제.개정내역
v1.00	2012년 11월	o “공인인증서를 이용한 본인확인 서비스 가이드라인” 제정