무선 공인인증서비스
사용자 인터페이스 가이드라인

User Interface Guideline for the Wireless Certificate Services

v1.0

2005년 12월

KISA 한국인터넷진흥원
Korea Internet & Security Agency

목 차

무선 공인인증서비스 사용자 인터페이스 가이드라인

User Interface Guideline for the Wireless Certificate Services

1. 개 요

본 가이드라인은 전자서명법 상에서 구축된 전자서명인증체계에서 공인인증기관이 발급한 무선 공인인증서비스의 상호연동성 확보 및 무선 단말기에서의 공인인증서(이하 인증서) 이용 편의성 제고 방안 등을 권고한다.

2. 구성 및 범위

본 가이드라인은 무선 인증서 상호연동을 대비하여 사용자 인터페이스 초기 표시 방법, 저장매체별 저장 및 이용방법 등 상호연동에 필요한 기술적 방안을 명시하고, 인증서 이용의 편의성 제고 측면에서 가입자 소프트웨어가 해당 응용에 적합한 인증서를 자동으로 선택하여 이용자에게 제시하는 인증서 자동선택기능에 대해 기술한다.

마지막으로 부록에서는 사용자 인터페이스 초기화면 구현의 예, 공인인증서 자동선택 기능 구현의 예를 제시한다.

3. 관련 표준 및 규격

3.1 국외 표준 및 규격

[WPKI]	OMA, WAP-217-WPKI, *Wireless Application Protocol Public Key Infrastructure Definition*, Version 24-Apr-2001
[WTLS]	OMA, WAP-261-WTLS-20010406-a, *Wireless Transport Layer Security*, Version 06-Apr-2001
[WAPX509]	WAP Forum Proposed Version 9-Mar-2000, WAP-211-X.509 : *WAP Certificate and CRL Profile*

[WAPWPKI] WAP Forum Proposed Version 3-Mar-2000, WAP-217-WPKI, : *Wireless Application Protocol Public Key Infrastructure Definition*

[WAPCrypto] WAP Forum Proposed Version 05-Nov-1999, *WMLScript Crypto Library*

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

3.2 국내 표준 및 규격

[TTA-120012] TTA, TTAS.KO-12.0012, *전자서명 인증서 프로파일 표준,* 2000

[TTA-120013] TTA, TTAS.KO-12.0013, *전자서명 인증서 효력정지 및 폐지목록 프로파일 표준,* 2001

[KCAC.SIVID] KISA, KCAC.SIVID v1.11, *식별번호를 이용한 본인확인 기술규격,* 2002

[KCAC.TS.DSCP] KISA, KCAC.TS.DSCP v1.10, *전자서명 인증서 프로파일 표준,* 2003

[KCAC.TS.DN] KISA, KCAC.TS.DN v1.10, *전자서명인증체계 DN규격,* 2003

[KCAC.TS.ACUG] KISA, KCAC.TS.ACUG v1.0, *전자서명인증체계 공인인증서 갱신규격,* 2003

[KCAC.TS.PKCS11] KISA, KCAC.TS.PKCS11 v1.0, *암호토큰을 위한 PKCS#11 프로파일 규격,* 2003

[KCAC.UI] KISA, KCAC.UI, "*공인인증기관간 상호연동을 위한 사용자 인터페이스 기술규격*", 2001년 10월, http://www.rootca.or.kr

3.3. 기타

해당사항 없음

4. 정의

4.1 전자서명법 용어 정의

본 가이드라인에서 사용된 다음의 용어들은 법률 제6585호 및 동법 시행령에 정의되어 있다.

가) 인증서
나) 공인인증서
다) 공인인증기관
라) 공개키
마) 가입자
바) 전자서명인증관리체계
사) 이용자
아) 가입자 설비(가입자 소프트웨어)

4.2 용어의 정의

본 가이드라인을 위하여 다음과 같은 용어들을 정의한다.

가) 인증기관 식별자 : 인증서 DN의 O(Organization) 값

5. 약어

본 규격에서는 다음의 약어가 이용된다.

가) DN : Distinguished Name, 식별명칭
나) PKI : Public Key Infrastructure, 공개키 기반구조
다) CN : Common Name, 일반명칭
라) SDRAM : Synchronous Dynamic Random Access Memory, 동기식 동적 램
마) WAP : Wireless Application Protocol, 무선 응용 통신규약
바) OID : Object IDentifier, 객체 식별자
사) PIN : Personal Identification Number, 개인 식별 번호

6. 저장매체별 무선 인증서 저장 및 이용

6.1 저장매체

사용자가 무선 인증서를 저장할 수 있는 매체로는 <표 1>에서 정의한 바와 같이 내장 메모리, 스마트카드가 있다.

<표 1> 무선 공인인증서 저장매체 종류

인증서 저장위치	설 명
· 내장 메모리	· 무선 단말기에 내장되어 있는 메모리
· 스마트카드	· 무선 단말기에서 장착하여 사용하며, 집적회로를 포함한 카드

핸드폰 내장 메모리는 핸드폰 내부의 물리적인 메모리로 Flash ROM이나 SDRAM 등의 저장매체를 말한다.

6.2 저장 및 이용방법

본 가이드라인에서는 인증서가 무선 단말기의 내장 메모리에 저장되는 경우, 인증서 저장위치는 언급하지 않는다. 국내 무선 전자서명인증체계에서는 WAP의 WMLScriptCrypto 규격에 의한 signText 함수를 이용하므로, 인증서 저장위치와 관계없이 signText 함수를 통해 공인인증서를 이용할 수 있는 인터페이스를 제공함으로써 인증서 상호연동이 가능하다.

스마트카드에 공인인증서를 저장할 경우, "암호토큰을 위한 PKCS#11 프로파일 규격"을 준용하여야 한다.

<표 2> 저장매체별 인증서

인증서 저장위치	저장매체의 인증서 이용 방안
· 내장 메모리	WMLScriptCrypto 규격의 signText 함수 이용
· 스마트카드	"암호토큰을 위한 PKCS#11 프로파일 규격" 준용

7. 초기화면상의 인증서 표시방법

초기화면상의 인증서 표시 방법은 사용자 무선 단말기의 내장 메모리에 저장된 모든 인증서를 자동으로 검색하여 보여주되, 해당 공인인증기관에서 발행한 인증서에 우선 순위를 부여할 수 있다. 또한, 스마트카드에 저장된 공인인증서 이용을 위해 다른 저장매체를 선택할 수 있는 별도의 메뉴를 마련하여야 한다.

초기 사용자 인터페이스 구현의 예는 부록 1. 사용자 인터페이스 초기화면의 예를 참고한다.

8. 무선 공인인증서 사용자 인터페이스 개선

8.1 공인인증서 자동 선택 기능

PKI 응용에서 이용자가 전자서명을 위해 전자서명에 이용할 인증서를 선택하고 해당 인증서의 암호화된 전자서명키 사용을 위해 복호화 비밀번호를 입력하는 절차는 전자서명 수행을 위해 반드시 필요한 절차이다. 그러나, 사용자 인터페이스가 불편한 무선 단말기에서 공인인증서 선택 및 비밀번호를 입력하는 것은 이용자의 불편을 초래할 수 있다. 따라서, 공인인증서 자동 선택 기능을 이용하여 인증서 선택 절차를 생략함으로써 이용자 편의성을 제고시킬 필요가 있다.

공인인증서 자동 선택 기능이란 무선 PKI 응용에서 가입자 소프트웨어가 무선 단말기 내장 메모리에 저장된 인증서 중 해당 용도에 맞는 인증서를 이용자의 개입없이 자동 선택하여 이용자에게 제시하는 기능을 말한다. 즉, 가입자는 무선 PKI 응용 이용 시, 인증서 선택화면 없이 가입자 소프트웨어가 자동으로 선택하여 제시하는 인증서를 확인하고 해당 인증서의 비밀번호만 입력함으로써 보다 편리하게 무선 PKI 응용 서비스 이용이 가능하다.

인증서를 자동으로 선택 방법은 구현에 따라 다를 수 있다. 인증서 자동 선택 방법 중의 하나로 가입자 소프트웨어가 무선 단말기 내에 저장된 인증서를 모두 검색하여 인증서 내 'Policy Identifier'의 OID를 확인하여, 해당 응용에 적합한

OID를 가진 인증서를 선택하는 제시하는 방법을 사용할 수도 있다.

무선 PKI 응용에서 인증서 자동 선택 기능을 통해 인증서가 선택되는 경우, 인증서 선택을 위해 인증서가 표시하는 초기 화면은 필요 없다. 그러나, 이용자는 전자서명에 이용하는 인증서의 정보를 알고 있어야 하므로, 인증서 비밀번호 입력 화면에서 자동으로 선택된 공인인증서의 정보를 제공하여 이용자가 전자서명에 이용하는 인증서를 알 수 있도록 하여야 한다. 또한, 인증서 자동 선택 기능을 제공하더라도, 사용자가 자동 선택된 공인인증서 이외의 다른 인증서를 이용할 수 있도록 메뉴를 제공하여야 한다.

스마트카드에 저장된 인증서를 이용하기 위해서는 PIN 등을 입력하여야 하므로, 인증서 자동 선택 기능의 대상이 되는 인증서는 무선 단말기 내장 메모리에 저장된 인증서만으로 한정할 수 있다.

만약, 무선 단말기 내장 메모리에 응용의 용도에 적합한 서로 다른 인증서가 2개 이상 존재하는 경우에는 우선 순위를 정하여 2개의 인증서 중 하나의 인증서를 선택하거나, 8절의 초기 표시 화면을 통해 사용자가 이용할 공인인증서를 선택할 수 있도록 할 수 있다. 예로서, 무선 단말기 내장 메모리에 범용 인증서와 용도제한용 인증서가 공존하는 경우, 범용 인증서를 우선적으로 선택할 수 있다. 또한, 인증서 정책 OID가 동일한 인증서가 2개 이상 존재하는 경우, 8절의 초기 표시 화면을 통해 사용자가 이용할 공인인증서를 선택할 수 있도록 할 수 있다.

가입자 소프트웨어가 무선 단말기의 내장 메모리에 저장된 공인인증서 검색하여 적합한 용도의 인증서를 발견하지 못한 경우, 에러 메시지와 함께 응용을 종료하거나, 스마트카드에 저장된 인증서를 이용할 수 있는 메뉴를 제공할 수 있다.

무선PKI 응용에서 인증서 자동선택 구현의 예는 부록 2. 인증서 자동선택 화면의 예를 참고한다.

부록 1. 사용자 인터페이스 초기화면의 예

<초기화면 구성의 예>

□ 초기화면 구성

가입자 소프트웨어의 초기화면에서 사용자에게 표시하여야 하는 정보는 다음과 같다.

o 인증서 저장위치

- 인증서 저장위치는 무선 단말기의 내장 메모리, 스마트카드에 있으며 사용자가 선택 지정할 수 있는 기능 제공

o 인증서 정보

- 가입자가 인증서의 정보를 알 수 있도록 다음의 사항을 표시하여야 한다. 다만, 단말기 화면이 제약이 있는 경우, 초기화면에서는 인증서 소유자명만을 표시하고 문자열의 횡 스크롤이나 인증서 보기 메뉴를 통한 팝업 화면(또는 인증서 정보 표시 화면)을 통해 기타 정보를 표시할 수도 있다.

・인증서 소유자명 : 사용자의 인증서 CN (인증서정보 이용)
※ 기관인 경우 기관의 실명 또는 인증기관 식별자로 표시
・인증서 유효기간 : 인증서 유효기간을 알 수 있도록 인증서 만료일 또는 유효기간 표시
・발급기관 : 공인인증기관의 실명(인증서정보 이용)으로 표시
・인증서 용도 : 공인인증서의 용도 표시
※ 예) 범용, 용도제한용
・기타 인증서 관련 정보

o 다른 저장매체 선택 기능

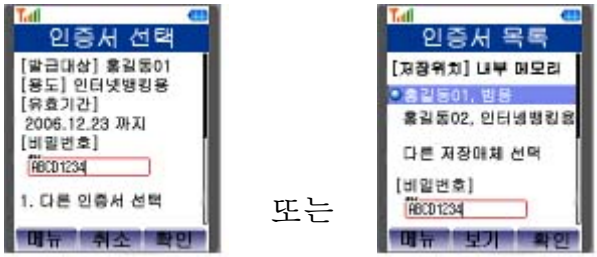
- 사용자가 임의로 다른 저장매체를 지정 후 인증서를 선택할 수 있는 메뉴

□ 인증서 정보보기 화면 구성의 예

무선 단말기 화면 제약으로 인해 초기화면에서는 인증서 소유자명만을 표시하고 인증서 보기 메뉴를 통한 팝업 화면(또는 인증서 정보 표시 화면)을 통해 기타 정보를 표시한 화면의 예들을 보여준다.

<초기화면에서 인증서 정보보기 메뉴 선택 시 화면 구성의 예>

부록 2. 공인인증서 자동 선택 기능 구현의 예



<인증서 자동 선택 기능 구현의 예>

□ 화면 구성

o 공인인증서 정보

- 인증서의 소유자 등을 확인할 수 있는 다음 정보 표시 기능 제공.
  · 인증서 소유자명 : 사용자의 인증서 CN (인증서정보 이용)
    ※ 기관인 경우 기관의 실명 또는 인증기관 식별자로 표시
  · 인증서 용도 : 공인인증서의 용도 표시.
    ※ 예) 범용, 용도제한용
  · 인증서 만료일 : 인증서 만료일을 알 수 있도록 만료일 또는 유효기간 표시

- 단말기 화면이 제약이 있는 경우, 초기화면에서는 인증서 소유자명만을 표시하고 문자열의 횡 스크롤 등을 통해 기타 정보 표시 가능

o 다른 인증서 선택하기

- 사용자가 자동으로 선택된 인증서를 이용하지 않고 다른 인증서를 이용하고자 하는 경우, 단말기 내장 메모리에 저장된 타 공인인증서나 스마트카드와 같은 다른 저장매체에 저장된 공인인증서를 불러오는 기능

□ 실제 응용에서 구현 예

① 무선 PKI 응용에서 인증서 자동선택이 구현된 예

② 사용자가 자동적으로 선택된 인증서 이외의 다른 인증서 이용하는 경우 등에는 인증서 초기화면을 표시하여 사용자가 직접 인증서 선택 가능

<1번 메뉴 선택> <초기화면표시>