공인인증기관간 상호연동 기술규격

Interoperability Specification
for Accredited Certification Authorities

[v1.00]

제 1 절 인증서 규격 관련사항

구분	주요 항목	권고 사항
인증서 규격 관련사항	인증서 및 CRL 형식	· DER, PEM 타입의 인증서를 처리할 수 있어야 함
	한글 UTF8 코딩 방식	· 인증서내 DN등에 사용되는 한글을 UTF8 형식으로 표현해야 함
	인증서 DN 형식	· 사용자 소프트웨어는 인증서내 UTF8 형식으로 표현된 한글 DN을 처리할 수 있어야 함 · 사용자 소프트웨어는 디렉토리 서버내 UTF8 형식으로 표현된 엔트리의 한글DN를 검색할 수 있어야 함
	인증서 소유자 신원정보	· 인증서 소유자의 실명은 한글로 인증서내 SubjectAltName 확장필드에 UTF8 문자열로 표현해야 함 · 인증서 소유자의 주민등록번호는 인증서내 SubjectAltName 확장필드의 OtherName 속성에 전자적인 방법으로 처리한후 표현해야 함

제 2 절 인증서 관리방식 관련사항

인증서 관리방식 관련사항	사용자 소프트웨어 설치	· 사용자 소프트웨어는 타 공인인증기관의 사용자 소프트웨어가 설치되는 디렉토리와 다른 위치에 생성되어야 함
	전자서명키 저장 방식	· 전자서명생성키는 PKCS #5 형식으로 암호화된 후 PKCS #8 형식으로 저장되어야 함
	전자서명키와 인증서 전달 방식	· 전자서명키와 인증서를 타 공인인증기관의 사용자 소프트웨어에서 Import/Export 하기 위하여 PKCS #12 형태로 생성되어야 함
	신뢰당사자의 인증서 및 CRL 획득 방식	· 타 공인인증기관의 인증서를 획득하기 위해 사용자 소프트웨어는 자체적인 테이블 형태로 획득 정보를 유지하거나 인증서 확장필드의 AIA 확장필드를 사용해야 함 · 타 공인인증기관의 CRL을 획득하기 위해 사용자 소프트웨어는 CRL DP 확장필드를 처리할 수 있어야 함

제 3 절 인증서 검증방식 관련사항

인증서 검증방식 관련사항	인증서 검증 방식	· 인증서 검증시에는 RFC2459의 절차를 준용하여 기본검증 및 각 확장필드가 가능해야 함 · 검증절차에는 Certificate Policies 확장필드를 무조건 검사하여 없으면 중단하는 절차를 포함하여야 함

제 4 절 인증서 검증방식 관련사항

디렉토리 서버 관련사항	디렉토리 스키마	· 인증서 및 CRL 저장공간 명칭은 RFC2587를 준용하여야 함 · 인증서는 userCertificate;binary, CRL은 certificateRevocationList;binary에 저장하여야 함
	디렉토리 DN 형식	· 디렉토리 엔트리의 DN 및 속성에 한글을 사용할 경우 한글을 UTF8 문자열로 표현해야 함