나. X.509 인증서 필드용도

다음은 X.509 인증서에서 사용되는 필드들에 대한 용도를 보여준다.

[표 10] X.509 인증서 필드용도

항목명	선택여부	설명
기본 정보		
Version	필수	인코딩된 인증서의 버전을 기술
Serial Number	필수	CA가 각 인증서에 지정한 정수
Signature Algorithm	필수	인증서를 서명하는 데 이용되는 알고리즘에 대한 알고리즘 식별자
Issuer	필수	인증서를 서명하는 기관의 유일 식별자 (X.500 고유 이름)
Validity	필수	인증서가 유효한 기간
Subject	필수	인증서 주체의 유일 식별자(X.500 고유 이름). DN (distinguished name)
Subject Public Key Info	필수	공개키와 그 키가 사용될 알고리즘을 식별
Unique Identifiers	선택	발행자 또는 subject 이름
확장 정보		
Authority Info Access	옵션	인증서 발급자의 위치정보
Authority Key Identifier	옵션	발급자의 키를 나타낼 수 있는 키의 식별자
Basic Constraints	옵션	제약 사항. 주로 이 인증서가 다른 인증서를 발급할 수 있는 권한이 있는지 없는지를 나타냄
Certificate Policies Ext	옵션	인증서 정책을 기술하고 있는 곳의 위치정보
CRL Distribution Points	옵션	이 인증서의 CRL 획득 위치
Ext Key Usage	옵션	인증서의 사용용도. OCSP 서명
Issuer Alt Name	옵션	발급자의 다른 이름. DN이외에 도메인 네임 사용 가능
Key Usage	옵션	인증서의 사용용도. 서명, 부인방지, 전자 서명, 키교환 등
Name Constraints	옵션	발급되는 인증서들의 DN에 사용될 이름에 대한 도메인 제한 정보
OCSP No Check	옵션	OCSP에서 서명된 인증서에 대해 OCSP에 대한 검증 요청이 필요 없음을 표시
Policy Constraints	옵션	인증서 경로의 제약 사항
Policy Mappings	옵션	IssuerDomainPolicy와 subjectDomainPolicy들에 대한 쌍으로 이루어진 Issuer와 Subject CA간의 정책 매핑
Private Key Usage Period	옵션	인증서와 별도로 공개키에 대응되는 개인키에 대한 사용 가능 기간
Subject Alt Name	옵션	Subject의 다른 이름. DN이외에 도메인 네임 사용 가능
Subject Key Identifier	옵션	공개키에 대한 식별자. 하나의 Subject Name으로 복수의 공개키가 발급된 경우 사용