□정보산업동향□

인증서 및 인증서 폐지목록 프로파일 동향

정 권 성† 이 재 일††

◈ 목 차 ◈

1. 서 론

1988년 ITU-T에서 디렉토리 표준 규격인 X.500 시리즈를 발표하면서 인증구조에 대한 부분으로 X.509가 발표되었고 이후 ISO와 함께 지속적으로 개정작업이 이루어졌으며 차후 버전에 대해서도 검토가 이루어지고 있는 상태이다.[7] ITU-T 및 ISO의 표준화가 지속적으로 이루어짐에 따라 인증서를 이용한 인증의 활용에 대한 필요성이 증가하게 되었고 이러한 요구는 인터넷에서의 공개키 기반구조 규격을 제정하는 IETF PKIX 작업그룹에서도 받아들여져 인터넷상에서의 공개키 기반구조에서 사용되는 인증서 및 인증서폐지목록에 대한 규격이 1999년 1월 발표되었다.[2]

인증서 규격은 기본적으로 모든 필드의 내용과 표현 가능한 데이터 형식 등에 대하여 기술하고 있지만 이러한 내용들이 인증서를 사용하고 활용하는 영역 또는 서비스에 따라서 일괄적으로 적용되는 것은 아니다. 따라서 서비스영역 내에서는 영역내의 인증체계 및 목적에 따라 다양하게 인증서 규격을 재정의하여 사용할 수 있으며 이를 기반으로 영역내의 인증체계를 유지하게 된다. 물론 인증서 규격을 재정의 함에 있어서 기존의 인증서 규격을 벗어나는 범위가 아니라 기존 인증서 규격을 준용하는 범위 내에서 이루어지게 된다. 이것을 기존의 인증서 표준 규격과 구분하여 인증서 프로파일이라고 한다. IETF의 인증서 및 인증서 폐지목록 규격도 마찬가지로 인터넷이라는 영역 내에서의 인증체계를 위한 별도의 프로파일이라 해석할 수 있다.

현재 인증서 및 인증서폐지목록에 대한 프로파일 작업은 국가별, 단체별, 서비스 영역별로 활발하게 이루어지고 있으며 이후 2절 및 3절에서는 주요 인증서 및 인증서폐지목록 프로파일 현황을 국제표준과 비교하여 소개하며 4절에서는 국내에서의 인증서 및 인증서폐지목록에 대한 프로파일 현황을 살펴본다.

2. 인증서 프로파일 동향

인증서 프로파일은 해당 서비스 영역 내에서 기존 규격을 기반으로 재정의하여 사용되는데 주로 인증서 검증 및 인증경로 검증을 위한 사항과 이에 대한 제약사항들을 명시하게 되며 이는 대부분 인증서확장필드에 관련된 사항들로 주요 항목으로는 다음과 같은 것들이 있다.

- 생성여부 : 인증서 생성시 해당 확장필드를

† 정회원 : 한국정보보호센터 연구원
†† 정회원 : 한국정보보호센터 선임연구원

포함하여 생성할 것인지를 결정함

- 처리여부 : 인증서 검증시 사용자 소프트웨어가 해당 확장필드를 처리할 수 있도록 할 것인지를 결정함
- 중요도(Criticality) : 인증서 생성시 해당 확장필드에 중요성을 부여하여 인증서 검증시 처리할 수 있는 경우에만 인증서를 받아들이도록 명시함

IETF RFC 2459 인증서 프로파일

IETF에서는 PKIX 실무자 작업 그룹을 통하여 인터넷 공개키 기반구조 상에서 사용되는 인증서 프로파일을 1999년 1월 RFC 2459로 정의하였다.[2] RFC 2459는 기본적인 규격에 대해서는 ITU-T의 X.509 과 동일하지만 구체적인 운영이나 생성 및 확장필드의 중요도 정도를 독자적으로 표현하고 있으며 인증경로 검증 부분에 대해서도 별도로 정의하고 있다. 이후 인증경로 검증 부분에 대한 수정 등으로 인하여 다음 버전의 규격이 IETF PKIX 실무자 작업그룹에서 논의되고 있으며 1999년 10월 드래프트버전이 발표된 상태이다.[8]

미국 FPKI(Federal PKI) 인증서 프로파일

미국 FPKI 인증서 프로파일에 대한 표준화 작업은 NIST의 공개키기반구조 실무자 작업반에서 수행하고 있으며 정기적인 모임을 통하여 FPKI에 대한 주요 쟁점사항들을 도출하여 이를 해결해 나가고 있다. 인증서 프로파일도 그 중 하나로 지속적으로 이에 대한 논의가 이루어지고 있다. 최초 FPKI에서의 인증서 프로파일은 일반 CA에 대한 부분에 대해서만 이루어져왔지만[9], 이후 키 관리용 인증서 및 Self-signed 인증서에 대한 프로파일이 정의되었고[4] 최근에는 Bridge CA에 대한 프로파일이 추가되어 발표되었다.[3]

미국 FPKI 인증서 프로파일은 IETF의 RFC 2459에서 정의하고있는 프로파일과의 관계를 검사하여 호환성 관련 문제를 조사하고 이를 차기 버전에 반영해나가고 있는 상황이다.

독일 인증서 프로파일

독일은 현재 전자서명법이 시행되어 이에 따라 전자서명 인증관리체계가 구축되어 있는 상태로 기술적인 측면과 더불어 법, 제도, 정책적으로도 많은 작업이 이루어져 있는 상태이다. 독일의 인증서 프로파일은 독일전자서명법에 의거하여 문서화 되었으며 IETF나 FPKI와는 달리 독일 내에서 사용되는 독자적인 프로파일을 정의하였다.[5][6]

독일 전자서명 인증관리체계는 최상위인증기

기본필드명	ITU-T1)		IETF2)		FPKI3)		독일4)	
	생성	처리	생성	처리	생성	처리	생성	처리
Version	m	m	m		m	m	m	
Serial Number	m	m	m		m	m	m	
Signature	m	m	m		m	m	m	
Issuer	m	m	m		m	m	m	
Validity	m	m	m		m	m	m	
Subject	m	m	m		m	m	m	
Subject Public Key Info	m	m	m		m	m	m	
Issuer Unique ID	o	o	x		o	o	x	
Subject Unique ID	o	o	x		o	o	x	
Extensions	m	m	m		m	m	m	

확장필드명	ITU-T			IETF			FPKI			독일		
	critical	선택여부		critical	선택여부		critical	선택여부		critical	선택여부	
		생성	처리		생성	처리		생성	처리		생성	처리
Authority Key Identifier	n	m	o	n	m		n	m	o	n	m	
Subject Key Identifier	n	m	o	n	m		n	m	o	n	o	
Key Usage	c	m	m	c	m		c	m	m	c	m	
Private Key Usage Period	n	o	o	n	x		n	x	o	c	o	
Certificate Policies	n	m	m	5)			c	m	m	n	m	
Policy Mappings	n	m	m	n	o7)		n	m7)	m	n	o7)	
Subject Alternative Names	both	m	m	both	o		n	o	m	n	m	
Issuer Alternative Names	both	m	m	n	o		n	o	m	n	o	
Subject Directory Attributes	n	o	o	n	x		n	o	o	n	o	
Basic Constraints	c	m	m	c	m7)		c	m	m	c	m	
Name Constraints	c	m7)	m	c	m7)		c	m7)	m	c	x	
Policy Constraints	c	m7)	m	both	o7)		c	m7)	m	c	x	
Extended Key Usage	both	o	o	both	o		n	x	o	8)		
CRL Distribution Points	both	m	m	n	m		9)	m	m	n	o	

c : critical n : non-critical both : critical or non-critical m : mandatory o : optional x : forbidden or not recommended

1) ITU-T Recommendation X.509(1997) | ISO/IEC 9594-8:1997, Information technology-Open Systems Interconnection- The Directory : Authentication framework

2) IETF RFC 2459 Internet X.509 Public Key Infrastructure, 1999. 1

3) Federal Public Key Infrastructure(PKI) X.509 Certificate Profile TWG-00-01, 2000. 1
- 인증서 각 필드의 처리부분은 TWG-99-01을 근거로 함

4) BSI Specification for Interoperable procedure and Components acording to SigG/SigV Signature-Interoperability Specification SigI : A1 Certificate, 1999. 1. 31

5) RFC 2459에서는 Criticality 또는 생성 시 포함여부에 대하여 특별히 권고하고 있는 사항이 없음

6) Critical인 경우에는 필수로 처리함

7) 최종 사용자용 인증서에는 사용하지 말 것을 권고함

8) CA용 인증서 및 최종 사용자용 인증서에는 사용하지 말 것을 권고함

9) Criticality는 인증서 폐지를 구현하는 방법에 따라 달라짐

관, 공인인증기관, 사용자로 구성되는 2 계층 인증구조로 이루어져 있으며 따라서 주요제약조건 중 Naming Constraint, Policy Constraint 등이 사용되지 않는다. 일반 CA 인증서 프로파일과는 별도로 시점확인용과 디렉토리용 인증서에 대한 프로파일을 정의하고 있는 점이 특이하다. 또한 독일의 인증서 프로파일에서는 인증서 생성 및 중요도에 관련된 부분을 중심으로 정의하고 있으며 인증서 처리에 대해서는 정의하고 있지 않다.

다음은 각국의 기관별 인증서 프로파일 중 일반적인 CA 인증서 프로파일을 기준으로 조사된 것이다.

3. 인증서 폐지목록 프로파일 동향

인증서 검증 및 인증경로 검증시 반드시 요구되는 사항중에 하나가 해당 인증서의 상태정보를 확인하는 것이다. 이를 위해서는 기본적으로 표준이나 프로파일에서는 인증서 폐지목록을 사용하는 것을 정의하고 있다. 인증서 폐지목록은 기본필드와 인증서폐지목록 확장필드로 구분되며 기본필드에는 중 폐지된 각각의 인증서에 대한 확장필드인 엔트리 확장필드가 포함된다.

인증서폐지목록 프로파일은 인증서 프로파일과

기본필드명	ITU-T1)		IETF2)		FPKI3)		독일4)	
	생성	처리	생성	처리	생성	처리	생성	처리
Version	m	m	m		m	m	m	
Signature	m	m	m		m	m	m	
Issuer	m	m	m		m	m	m	
This Update	m	m	m		m	m	m	
Next Update	m	m	m		m	m	m	
Revocated Certificates	m	m	m		m	m	m	
User Certificates	m	m	m		m	m	m	
Revocation Date	m	m	m		m	m	m	
CRL Entry Extionsions	m	m	m		m	m	m	
CRL Extensions	m	m	m		m	m	m	

인증서효력정지 및 폐지목록 확장필드명	ITU-T			IETF			FPKI			독일		
	critical	선택여부		critical	선택여부		critical	선택여부		critical	선택여부	
		생성	처리		생성	처리		생성	처리		생성	처리
Authority Key Identifier	n	m	o	n	m		n	m	o	n	m	
Issuer Alternative Name	n	m	m	n	o		n	m	m	n	o	
CRL Number	n	m	o	n	m		n	m	o	n	m	
Issuer Distribution Point	c	m	m	c	o		c	m	m	c	x	
Delta CRL Indicator	c	o	o	c	o		n	o	o	c	o	

엔트리 확장필드명	ITU-T			IETF			FPKI			독일		
	critical	선택여부		critical	선택여부		critical	선택여부		critical	선택여부	
		생성	처리		생성	처리		생성	처리		생성	처리
Reason Code	n	m	o	n	m		n	m	o	n	o	
Hold Instruction Code	n	o	o	n	o		n	o	o	n	x	
Invalidity Date	n	m	o	n	m		n	m	o	n	x	
Certificate Issuer	c	m	m	c	m		c	m	m	c	x	

c : critical n : non-critical both : critical or non-critical m : mandatory o : optional x : forbidden or not recommended

1) ITU-T Recommendation X.509(1997) | ISO/IEC 9594-8:1997, Information technology-Open Systems Interconnection- The Directory : Authentication framework

2) IETF RFC 2459 Internet X.509 Public Key Infrastructure, 1999. 1

3) Federal Public Key Infrastructure(PKI) X.509 Certificate and CRL Extensions Profile TWG-99-01, 1999. 1

4) BSI Specification for Interoperable procedure and Components according to SigG/SigV Signature-Interoperability Specification SigI : A5 Notice Service, 1999. 1. 31

마찬가지로 해당 서비스 영역 내에서 기존 규격을 기반으로 재정의하여 사용되며 인증서 상태정보 확인을 위한 방법 및 관련 정보를 명시하게 되고 다음과 같은 항목에 대해서 주로 정의하게 된다.

- 생성여부 : 인증서 효력정지 및 폐지목록 생성시 해당 확장필드를 포함하여 생성할 것인지를 결정함
- 처리여부 : 인증서 효력정지 및 폐지목록 처리 사용자 소프트웨어가 해당 확장필드를 처리할 수 있도록 할 것인지를 결정함
- Criticality : 인증서 효력정지 및 폐지목록 생성시 해당 확장필드에 중요성을 부여하여 인증서 검증시 처리할 수 있는 경우에만 인증서 효력정지 및 폐지목록을 받아들이도록 명시함

인증서 효력정지 및 폐지목록 프로파일은 해당 영역내에서 인증서 상태점증을 위한 수단으로 무엇을 사용할 것인가에 따라 많이 달라지며 이에 대하여 대부분의 프로파일에서는 ITU-T X.509 표준을 준용하고 있다.

4. 국내 전자서명 인증관리체계의 프로파일 동향

국내에서는 1999년 2월 전자서명법이 제정되고 1999년 7월 전자서명 인증관리센터가 개원하면서 전자서명 인증관리체계가 구축이 되었고 이후 국내 전자서명 인증관리체계에 맞는 인증서 프로파일을 개발하였다. 현재 최상위 인증기관의 Self-signed 인증서 및 공인인증기관의 인증서가 발급되어 있는 상태이며 인증서 상태정보 확인을 위해서는 인증서효력정지 및 폐지목록을 이용하고 이를 주기적으로 공고하고 있다.

다음은 전자서명 인증관리체계의 인증서 프로파일로서 Self-signed 인증서 및 공인인증기관 인증서 발급에 사용된다. 생성 및 처리에서 필수로 요구되는 확장필드는 전자서명 인증관리체계 유지를 위하여 최소한으로 요구되는 사항들이며 공인인증기관들은 이를 기준으로 최소한의 요구사항을 지키면서 추가적으로 자신의 영역에 맞는 확장필드를 선택하여 인증서 프로파일을 구성하면 된다.

전자서명 인증관리체계에서 사용하고 있는 인증서 효력정지 및 폐지목록은 다음과 같으며 이것을 이용하여 인증서 효력정지 및 폐지 여부를 확인할 수 있도록 한다. 이를 위하여 엔트리 확장필드의 Reason Code 필드를 이용하며 효력정지 사유 발생시 이 필드를 이용하게 된다. 인증서 프로파일과 마찬가지로 인증서 효력정지 및 폐지목록 프로파일 또한 국제표준을 준용하여 작성되며 미국 FPKI 및 IETF RFC 2459와도 호환성을 유지하도록 설정되어 있다.

기본필드명	KISA	
	생성	처리
Version	m	m
Serial Number	m	m
Signature	m	m
Issuer	m	m
Validity	m	m
Subject	m	m
Subject Public Key Info	m	m
Issuer Unique ID	o	o
Subject Unique ID	o	o
Extensions	m	m

인증서 확장필드명	KISA		
	critical	선택여부	
		생성	처리
Authority Key Identifier	n	m	o
Subject Key Identifier	n	m	o
Key Usage	c	m	m
Private Key Usage Period	n	o	o
Certificate Policies	both	m	o*
Policy Mappings	n	o	o
Subject Alternative Names	n	o	o
Issuer Alternative Names	n	o	o
Subject Directory Attributes	n	o	o
Basic Constraints	c	m	m
Name Constraints	c	o	o
Policy Constraints	c	o	o
Extended Key Usage	c	o	o
CRL Distribution Points	n	m	o

c : critical n : non-critical both : critical or non-critical m : mandatory o : optional x : forbidden
* : critical 인 경우에는 필수로 처리해야 함

기본필드명	KISA	
	생성	처리
Version	m	m
Signature	m	m
Issuer	m	m
This Update	m	m
Next Update	m	m
Revocated Certificates	m	m
User Certificates	m	m
Revocation Date	m	m
CRL Entry Extionsions	m	m
CRL Extionsions	m	m

인증서효력정지 및 폐지목록 확장필드명	KISA		
	critical	선택여부	
		생성	처리
Authority Key Identifier	n	m	o
Issuer Alternative Name	n	o	o
CRL Number	n	m	o
Issuer Distribution Point	c	o	o
Delta CRL Indicator	c	o	o

엔트리 확장필드명	KISA		
	critical	선택여부	
		생성	처리
Reason Code	n	m	m
Hold Instruction Code	n	o	o
Invalidity Date	n	o	o
Certificate Issuer	c	o	o

c : critical n : non-critical both : critical or non-critical m : mandatory o : optional x : forbidden

5. 결 론

현재 공개키기반구조 및 전자서명 인증관리체계를 구축하는 곳에서는 국제표준을 준용하면서 각 서비스 영역의 특성에 맞는 인증서 프로파일을 개발하는 것이 필수 조건이 되어 가고 있다. 인증서 프로파일은 인증서비스를 제공하기 위해 인증기관이 준비해야 하는 가장 기본적인 요소가 되었고 상호인증 등을 고려하는 경우라면 인증서 프로파일의 생성, 처리, 중요도 부분의 상관관계를 정확하게 설정해야하는 필요성이 더욱 커지게 된다.

국내 전자서명 인증관리체계 프로파일은 2계층 구조인 전자서명 인증관리체계 특성에 맞게 구성이 되었으며 국제 표준 및 기타 다른 인증서 프로파일과 최대한 호환성을 유지하고자 필수로 요구되는 부분들을 최소화하였다. 앞으로는 이에 대한 지속적인 연구가 이루어져 국내 표준으로 제정될 수 있도록 할 예정이다.

참고문헌

[1] ITU-T Recommendation X.509(1997) | ISO/IEC 9594-8:1997, Information technology-Open Systems Interconnection- The Directory : Authentication framework

[2] R. Housley, W. Ford, W. Polk, D. Solo, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC 2459, 1999. 1.

[3] Federal Public Key Infrastructure(PKI) X.509 Certificate Profile, TWG-00-01, 2000. 1.

[4] Federal Public Key Infrastructure(PKI) X.509 Certificate and CRL Extensions Profile, TWG-99-01, 1999. 1.

[5] BSI Specification for Interoperable procedure and Components acording to SigG/SigV Signature-Interoperability Specification SigI : A1 Certificate, 1999. 1. 31.

[6] BSI Specification for Interoperable procedure and Components according to SigG/SigV Signature-Interoperability Specification SigI : A5 Notice Service, 1999. 1. 31.

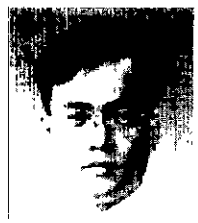
[7] ITU-T Recommendation X.509 | ISO/IEC 9594-8, Information technology-Open Systems Interconnection-The Directory : Public-Key and Attribute Certificate Framework (Editor's draft combining 97 text, FPDAM text, FPDAM restructure proposals and DTCs), 1999. 9.

[8] R. Housley, W. Ford, W. Polk, D. Solo, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, Draft, 1999. 10.

[9] Comparison of Public Key Certificate and Certificate Revocation List Profiles, TWG-98-56, 1998. 8.

정 권 성

1996년 성균관대학교 이과대학 수학과 졸업(학사)
1997년-1999년 성균관대학교 공과대학 정보공학과 졸업(석사)
1998년-현재 한국정보보호센터 연구원



이 재 일

1986년 서울대학교 계산통계학과 졸업(학사)
1986년-1988년 서울대학교 계산통계학과(석사)
1991년-1996년 한국 IBM 소프트웨어 연구소
1996년-현재 한국정보보호센터 선임연구원