효율적인 Delta-CRL 발급 시스템

현상우*, 김락현*, 이용**, 엄희정***, 염흥열*

*순천향대학교 정보보호학과,

**한국정보보호진흥원 전자서명인증관리센터

***KSIGN 정보보안연구소

Efficient Delta-CRL Issuing System

Sang-Woo Hyun*, Rack-Hyun Kim*, Yong Lee**, Hee-Jung Um***, Heung-Youl Youm*

*Department of Information Security Soonchunhyang Univ.,

**Korea Certification Authority Central, KISA

***KSIGN Research Institute

요 약

본 논문은 현재 국내에서 개발되고 있는 인증서 발급 시스템에서 인증서가 취소되었을 경우에 발급되는 인증서 취소목록(Certificate Revocation List : CRL)에 따른 문제점 중, 유통되는 트래픽 부하를 줄이고, 발급되는 CRL의 크기를 감소시키며, 또한 전체 CRL의 발급 시간을 연장시킬 수 있는 Delta-CRL 발급 시스템의 정책, 운영 방안 및 발급 방법을 제시한다. 제안된 운영 방안은 Full-CRL의 Distribution Point를 이용하여 Base-CRL을 가리키고 Base-CRL의 Delta-CRL distribution point를 이용하여 Delta-CRL의 위치를 확인한다. 그리고 세 가지 Delta-CRL 발급 시스템의 동작 방법들을 분석하였다.

I. 서론

주체가 인증서를 발행 받은 후, 인증서를 발행 받은 주체의 이름이 변경되거나, 주체가 인증서를 발행했던 조직에서 퇴직하거나 변동이 있거나, 인증서의 공개키에 대응되는 개인키가 누설되거나 도난당했을 경우에 주체에게 발행된 인증서를 폐지하게 된다. 이때 폐지된 인증서는 CRL 형태로 공개적으로 관리, 분배된다. 폐지된 인증서는 CRL에 그 내용을 목록화하여 발급함으로서, 해당 인증서가 불법적으로 사용되거나 도용되는 것을 방지할 수 있다. 그러나 인증서 발행의 수적 증가로 폐지된 인증서 또한 기하 급수적으로 증가하게 되고, 이는 분산된 통신상에서 트래픽의 증가와 CRL 데이터베이스의 저장 공간을 증가시키는 문제를 낳고 있다.[1]

Delta-CRL은 Full-CRL을 발행하는 것 보다 Full-CRL이 발행된 이후로 발생한 인증서 상태가 변경된 인증서들의 목록만을 포함한다.

제안된 시스템은 델타 CRL과 관련된 여러 문제를 해결하는 방법을 제시하고 있다. Delta-CRL을 Scope 별로 발행함으로써 CRL 데이터베이스의 저장 용량을 줄이는 방법을 제안한다. Scope 별로 발행함으로써 장점은 디렉터리 구조나 데이터베이스 상에서 CRL을 검색하여 조회하는 경우에 시간 손실을 줄일 수 있다.

본 논문에서는 Delta-CRL에서 필요한 확장자들에 관한 내용과 기존의 Delta-CRL을 발급하는 세 가지 방법에 대하여 분석하고, 현재까지 체계화되지 않았던 KISA(Korean Information Security Agency) Delta-CRL 발급 정책을 제시한다. 그리고 Scope 별 Delta-CRL 발행구조 및 시스템 구조를 정의하고 그에 따른 운영방안을 제안한다.

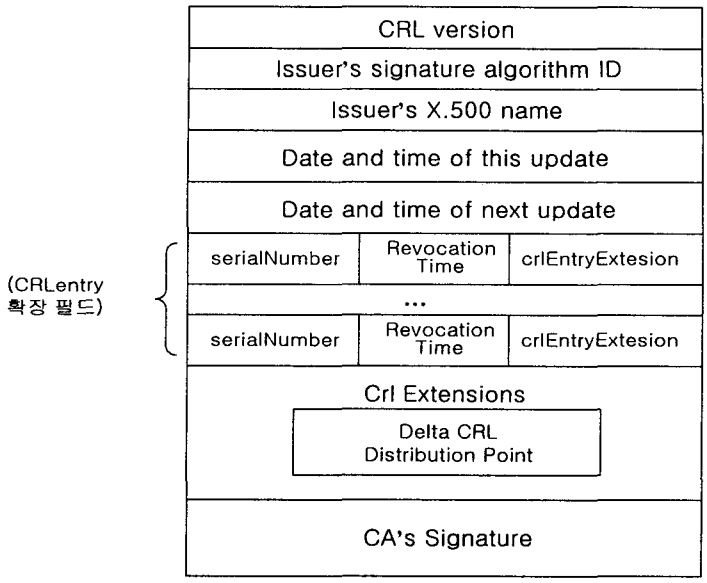

그림 1 : Base CRL의 확장자

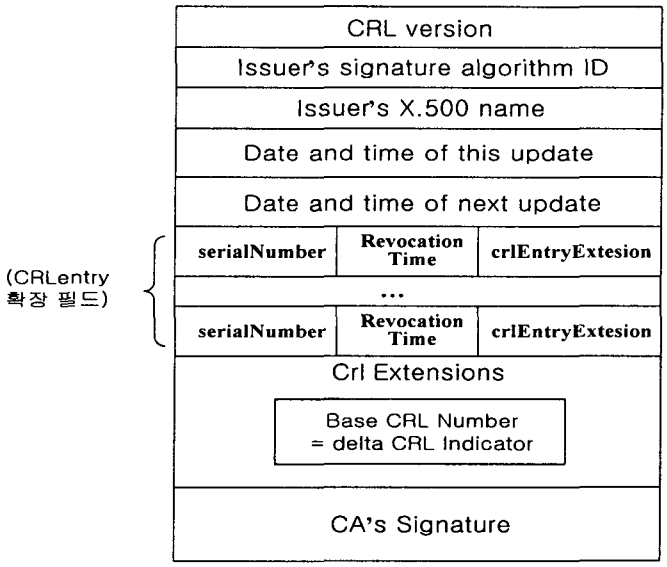

그림 2 : delta CRL의 확장자

II. Base-CRL 및 Delta-CRL의 확장자

본 장에서는 Base-CRL 및 Delta-CRL 관련 확장자를 분석한다. Delta-CRL을 발행 할 경우, 그에 따른 Base-CRL과 인증서와 같은 경우에는 Delta-CRL Indicator에 의해 Delta-CRL의 위치, 즉 Delta-CRL의 URL을 파악하여 발급을 받는다. 그림 1은 Base-CRL의 필드들을 나타낸 것이다. 그림에서 보는 바와 같이 Base-CRL은 CRL 확장 필드 내에 Delta-CRL distribution point라는 서브 필드를 포함하고 있어야 한다. 그림 2에서 알 수 있듯이 각각의 Delta-CRL은 Delta-CRL Indicator 역할을 하는 Base-CRL Number 필드를 포함하고 있다.

1. CRL Distribution Points

CRL 분배 점은 어떻게 CRL 정보를 획득할 것인지를 확인하는 확장자를 지적한다. 이 확장자는 non-critical 이다. 그러나 PKIX 프로파일에서는 인증기관들과 응용이 이 확장자를 지원할 것을 권고한다.

cRLDistributionPoints 확장자는 Distribution-Point의 SEQUENCE OF 타입이다. Distribution-Point는 URL 형태의 분배점을 포함하는 distributionPoint, 취소 범위를 나타내는 reasons, 그리고 cRLIssuer 등의 3개의 서브필드들로 다시 구성되는데, 각 서브필드는 선택적이다. 그러나, 이 필드들이 선택적이지만, DistributionPoint는 오직 reasons 필드만으로 구성되어서는 안된고, distributionPoint 또는 cRLIssuer 중 하나가 반드시 존재해야 하며, 인증서 발행자가 CRL 발행자가 아니면 cRLIssuer 필드는 반드시 존재해야 하고 CRL 발행자의 이름을 포함해야 한다. 만약 인증서 발행자가 CRL 발행자이라면, cRLIssuer 필드는 생략되어야 하고, distributionPoint 필드는 존재해야 한다. 만약 distributionPoint 필드가 생략된다면, cRLIssuer는 반드시 존재해야 하고, CRL이 위치하는 X.500 또는 LDAP 디렉토리 엔트리에 대응되는 이름을 포함해야 한다.[2][3]

2. Delta-CRL Indicator

Delta-CRL Indicator는 현재 CRL이 Delta-CRL임을 확인하는 critical 확장자이다. Delta-CRL은 취소된 모든 인증서 취소 목록을 가지고 있는 것이 아니라, 이전에 발행된 기반 CRL 이후에 상태가 변한 인증서 목록만을 포함한다. Delta-CRL의 사용은 어떤 환경에서 상당히 망 부하와 처리 시간을 줄일 수 있다. Delta-CRL은 일반적으로 Full-CRL보다 크기가 작다. 그러므로 Delta-CRL을 획득하는 것이 대응되는 Full-CRL을 획득하는 방법보다 망 대역폭을 감소시킬 수 있다.[4][5]

Delta-CRL Indicator 확장자는 BaseCRLNumber의 일련번호를 포함한다. 이 CRL 번호는 Delta-CRL을 생성하기 위한 시작점으로 사용된 주어진 범위에 대한 Base-CRL을 확인한다. CRL issuer는 참고된 Base-CRL을 Full-CRL로 공표한다. Delta-CRL은 동일한 범위에 대한 취소 상태의 모든 갱신 정보를 포함한다. Delta-CRL과 참조된 Base-CRL이 결합된 Full-CRL은 Delta-CRL이 공표된 시점에서 주어진 범위에 대한 Base-CRL과 등가이다.[4]

Delta-CRL은 Delta-CRL에 대응되는 Base-CRL과 동일한 범위를 갖는다. 즉, Delta-CRL의 범위는 기반으로 참조하는 완전한 CRL의 범위와 등가가 됨을 의미한다. 이 참조된 Base-CRL과 Delta-CRL은 distribution point 확장자를 제거해야 하거나 동일한 issuing distribution point 확장자를 포함해야 한다.[9]

3. issuing distribution point

issuing distribution point는 특정 CRL을 위한 CRL 분배점과 범위를 확인하기 위한 critical 확장자이다. 그리고 issuing distribution point는 이 CRL이 최종 개체만을 위한 취소인지, 인증기관만을 위한 취소인지, 또는 제한된 사유들의 집합을 갖는 취소인지를 나타낸다. 이 확장자는 critical 이지만 호환 실현은 이 확장자를 지원하도록 요구되지 않는다.[8]

분배점과 연관되는 사유 부호들은 onlySomeReasons 서브 필드에 규정되어야 한다. 만약 onlySomeReasons 가 나타나지 않는다면, 이 분배 점은 모든 사유 부호에 대한 취소를 포함해야 한다. 인증기관은 손상이나 정기적인 취소에 바탕을 둔 CRL을 다시 세부적으로 분할하기 위하여 CRL 분배 점들을 사용해야 한다. 이러한 경우, 사유 부호 keyCompromise(1)(개인키 누설), cACompromise(2)(인증기관 개인키 손상), 그리고 aACompromise(8)(속성 인증서 취소) 인 취소는 하나의 분배 점에서 나타나고, 다른 취소 사유들을 갖는 취소는 또 다른 분배점에서 나타낸다.[9]

III. CARL/CRL과 Delta-CARL/CRL 발급 정책

본 장에서는 KISA와 공인 인증기관에 적용 가능한 CRL과 Delta-CRL 관련된 인증서 정책을 제안한다. 이를 위하여 두 가지 인증서 취소 목록의 유형을 정의한다. 하나는 KISA가 공인 인증기관에게 발행한 인증서 중에서 취소된 인증서 목록을 나열한 것으로, KISA에 의하여 발행되는 공인 인증기관을 위한 인증기관 취소 목록(CARL:Certification Authority Revocation List)이다. 다른 하나는 공인 인증기관이 고객에게 발행된 인증서들 중에서 취소된 인증서 목록으로써, 공인 인증기관에 의하여 발행되는 인증서 취소 목록(CRL : Certification Revocation List)이다.

KISA는 CARL를 발행해야 하고, 공인 인증기관은 CRL을 발행해야 한다.

KISA는 선택적으로 Delta-CRL 발행을 지원할 수 있다. 공인 인증기관은 자신의 인증서 정책에

따라 선택적으로 Delta-CRL을 발행할 수 있다.

CARL 과 CRLs 내에 존재하는 내용은 포함되기 전에 철저히 검증되어야 한다. 검증은 부적절하게 생성된 CARL 또는 CRL에서 오류를 찾기 위한 소프트웨어를 이용하거나 다른 신뢰적인 수단을 이용하여 수행되어야 한다.

1. KISA CARL 또는 Delta-CARL 발행 주기

KISA는 공인 인증기관이 개인키 손상 사유로 인증서 취소를 요청하면, 공인 인증기관 인증서 취소 요구의 정당성을 확인하고, 요구를 수신시간부터 6시간 이내에 관련 취소 명단을 CARL에 공개해야 한다.

KISA는 정기적으로 발행되는 CARL과 개인키 손상으로 발행되는 CARL을 유지해야 한다. KISA는 공인 인증기관 CRL 정보를 시기 적절하게 당사자에게 제공하기 위하여 CRL을 취소 정보의 변경이 없을 때라도 주기적으로 발행해야 한다. KISA는 인증서 상태 정보를 표 1에서 규정된 발행 빈도보다 더 자주 발행해야 한다.

표 1 CARL 발행 주기

	정기적인 발행	개인키 손상으로 인한 발행
CARL	적어도 하루 한번	6시간

KISA는 정기적인 발행의 경우 하루에 한번씩 CARL을 발행해야 한다. 또한 KISA는 공인 인증기관의 개인키의 손상으로 인한 경우, 공인 인증기관에 의한 취소 요구를 수신한 후 6시간 이내에 개인키 손상 범위를 갖는 CARL을 발행해야 한다. KISA는 개인키 손상 CARL 요구사항을 만족하기 위하여 6시간마다 개인키 손상의 범위를 갖는 CARL을 발행하거나, 하루에 한번 CARL을 발행하고 6시간마다 Delta-CARL을 발행할 수 있다. 따라서 KISA는 두 범위에 대한 Delta-CRL을 선택적으로 발행할 수 있음을 의미한다.

공인 인증기관은 자신의 인증서 정책으로 CRL 발행 주기와 CRL 범위(scope)를 결정해야 한다.

CRL/CARL 은 계획된 다음 갱신 일시보다 빨리 발행되어야 한다. 신뢰 당사자는 오프라인으로 인증서 상태 정보를 자국에 저장할 수 있다. 이전 인증서 취소 목록은 최근 인증서 취소 목록으로 대체되어야 한다.

2. Delta-CARL/CRL 범위

KISA는 Delta-CARL을 선택적으로 지원한다. Delta-CARL 발행 주기는 6시간 단위로 한다. Delta-CARL의 범위(scope)는 전체 취소 사유와 개인키 손상으로 한정한다. 따라서 CRAL 역시 두 가지 범위로 발행한다.

공인 인증기관의 Delta-CRL 발행 정책은 공인 인증기관의 자율로 결정한다.

IV. Delta-CRL 운영방안

1. Delta-CRL 발급 시스템의 개요

제안된 발급 시스템의 구조는 그림 3과 같다.

▶ Delta-CRL 발급 시스템 구조

- 사용자가 인증기관으로부터 인증서를 발급 받음.
- 사용자가 인증서의 취소를 해당 인증기관에 인가된 방법으로 요청하면 인증기관은 CRL에 해당 인증서를 포함함.
- 인증서 발급 및 취소 방법은 PKIX 의 CMP 프로토콜을 이용함.

▶ Base-CRL 과 Delta-CRL 생성 방안

- Base-CRL 과 Delta-CRL 구조 : CRL 구조와 동일하나, DP(Distribution Point) 역할이 서로 다름.
- Client 는 Full-CRL을 얻기 위하여 Base-CRL과 Delta-CRL을 결합함.
- FULL-CRL과 Base-CRL 그리고 Delta-CRL은 디렉토리 서비스 또는 웹을 이용하여 공개함.

FULL-CRL을 구하기 위하여 Delta-CRL이 Base-CRL과 결합(Combine)될 때, Base-CRL은 Delta-CRL과 동일한 CRL number 번호 체계를 유지해야 한다. 또한, Base-CRL은 지금 발행 일시인 thisUpdate 와 다음 발행 예상 일시인 nextUpdate 필드를 갖는다. 거기에 더하여 Base-CRL은 issuing distribution point를 이용하여 특정 범위로 발행된 특정 범위의 델타 CRL을 확인할 수 있다.[7]

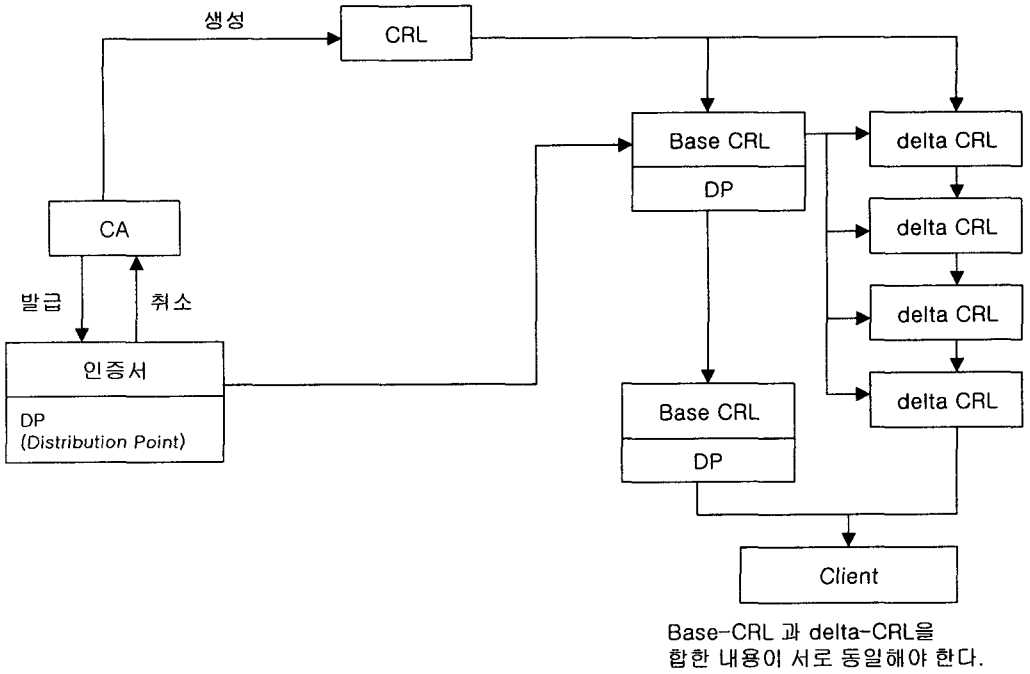

그림 3 : delta CRL 발급 시스템

▶ Base-CRL과 Delta-CRL은 다음 4가지 조건이 만족하면 결합된다.

- Base-CRL과 Delta-CRL이 동일한 발행자를 가진다.
- Base-CRL과 Delta-CRL은 동일한 범위를 갖는데, 두 CRL 들이 다음의 조건을 만족해야만 한다.
  - · issuingDistributionPoint 확장자가 Base-CRL과 Delta-CRL에서 공히 생략되어 있다.
  - · issuingDistributionPoint 확장자가 Base-CRL과 Delta-CRL에서 공히 존재하고, 확장자들에서 필드들의 각각의 값들이 동일하다.
- Base-CRL의 CRL 번호가 Delta-CRL에서 정의된 BaseCRLNumber 보다 같거나 커야 한다.
- Base-CRL의 CRL 번호가 Delta-CRL 번호보다 작아야 한다. 이는 Delta-CRL이 번호 순서에서 완전한 CRL을 따르는 것을 의미한다.

위의 Delta-CRL 발급시스템을 좀 더 자세히 살펴보면 그림 4와 같다.

2.1 절에서 설명했듯이 DistributionPoint 확장자를 살펴보면 distributionPoint, reasons, 그리고 cRLIssuer의 세 개의 필드로 구성되어 있음을 알 수 있다. 그 중에서 reasons 필드는 다음과 같은 취소 사유들을 포함하고 있다.

```
ReasonFlags ::= BIT STRING {
unused                  (0),  //사용 않함
keyCompromise           (1),  //키 손상
cACompromise            (2),  //인증기관 손상
affiliationChanged      (3),  //직장 변경
superseded              (4),  //지위 박탈
cessationOfOperation    (5),  //동작 중단
certificateHold         (6),  //인증서 유보
privilegeWithdrawn      (7),  //특권 취소
aACompromise            (8) } //속성인증서손상
```

만약 DistributionPoint가 reasons 필드를 생략하면, CRL은 모든 이유들을 갖는 취소 정보를 포함한다.

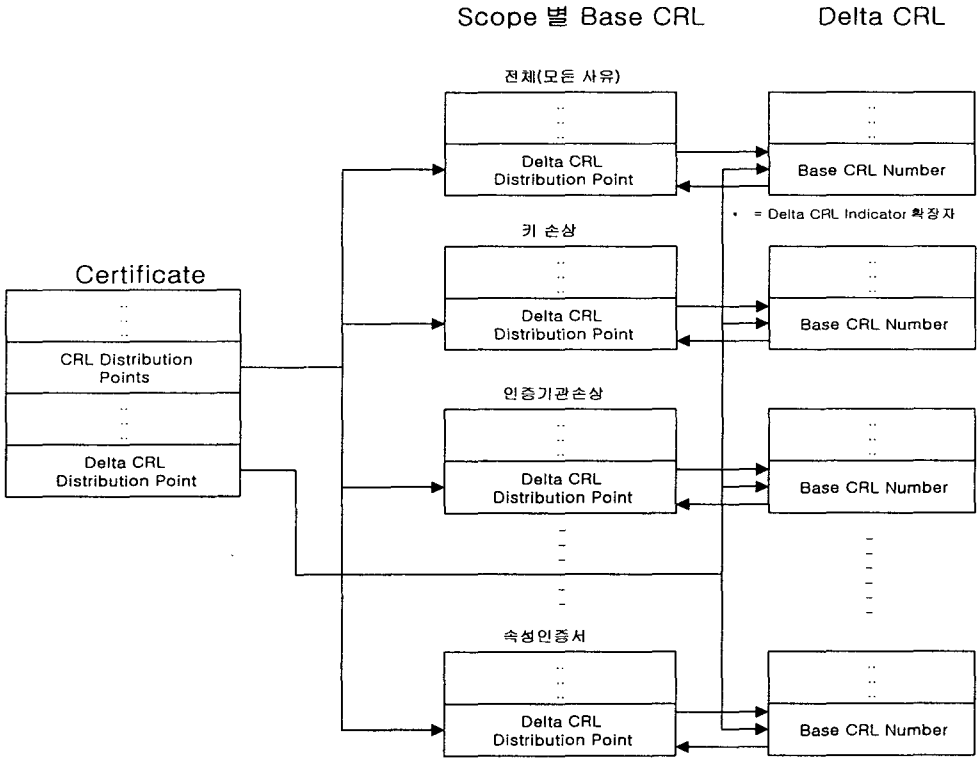

그림 4 : delta CRL 발급 시스템의 체계

Delta-CRL 발급 시스템의 운영 방침은 기본적으로 다음과 같은 원칙을 따른다.

▶ Delta-CRL 발급 시스템 운영 원칙

- CRL distribution point 확장자의 reasons 필드를 이용 Scope 별 Full CRL을 발행.
- 인증서에 Base-CRL을 지적하는 CRL Distribution Point와 Delta-CRL 지적하는 Delta-CRL Distribution Point 확장자를 이용하여 위치 확인.
- 각각의 Distribution Point는 CRL이 저장되어 있는 디렉토리 위치 또는 파일을 얻을 수 있는 URL 형태임.
- Base-CRL는 Delta-CRL Distribution Point 확장자를 가지고 있음.
- Base-CRL은 독립적인 번호 체계를 유지함.
- Delta-CRL은 자신이 참조하는 기반 CRL을 나타내기 위한 Base-CRL Number 확장 필드를 가지고 있음
- Base-CRL과 Delta-CRL의 발급은 다음 장부터 설명되는 방식으로 하되, 발행 간격 등은 인증기관 정책에 의하여 결정됨.

2. Delta-CRL 발급시스템의 동작방법

본 절에서는 지금까지 발표된 대표적인 세 가지 Delta-CRL 동작 방법을 분석한다. 첫 번째 방법은 Full-CRL은 3시간마다 한번씩 발행되고 Delta-CRL은 1시간마다 한번씩 발행되어 3시간마다 Delta-CRL의 Base-CRL 번호가 바뀌는 전형적인 방법이고, 두 번째 방법은 Full-CRL의 이력을 3시간에서 6시간으로 늘리는 슬라이딩 윈도우 방식을 채택한 방법, 그리고 세 번째 방법은 슬라이딩 윈도우 방식을 사용한 복사/전달 지연 시간을 고려하여 발행하는 방법이다.

아래의 세 가지 방법을 설명 효율적으로 설명하기 위하여 취소 사유에 대한 용어를 다음과 같이 정의하였다.

표 2 전형적인 Delta-CRL 발급 방법

Current time	Revoked certificates	Full CRL	Delta-CRL
12:00	{14k}	cRLNumber = 1 thisUpdate = 12:00 nextUpdate = 15:00 CertificateList = {14k}	cRLNumber = 1 thisUpdate = 12:00 nextUpdate = 13:00 BaseCRLNumber = 1 CertificateList = {}
13:00	{14k, 124k}		cRLNumber = 2 thisUpdate = 13:00 nextUpdate = 14:00 BaseCRLNumber = 1 CertificateList = {124k}
14:00	{14k, 124k}		cRLNumber = 3 thisUpdate = 14:00 nextUpdate = 15:00 BaseCRLNumber = 1 CertificateList = {124k}
15:00	{14k, 124k, 39h}	cRLNumber = 4 thisUpdate = 15:00 nextUpdate = 18:00 CertificateList = {14k, 124k, 39h}	cRLNumber = 4 thisUpdate = 15:00 nextUpdate = 16:00 BaseCRLNumber = 1 CertificateList = {124k, 39h}
16:00	{14k, 124k, 39h, 67a}		cRLNumber = 5 thisUpdate = 16:00 nextUpdate = 17:00 BaseCRLNumber = 4 CertificateList = {39h, 67a}
17:00	{14k, 124k, 67a}		cRLNumber = 6 thisUpdate = 17:00 nextUpdate = 18:00 BaseCRLNumber = 4 CertificateList = {39r, 67a}
18:00	{14k, 124k, 67a}	cRLNumber = 7 thisUpdate = 18:00 nextUpdate = 21:00 CertificateList = {14k, 124k, 67a}	cRLNumber = 7 thisUpdate = 18:00 nextUpdate = 19:00 BaseCRLNumber = 4 CertificateList = {39r, 67a}
19:00	{14k, 124k, 67k}		cRLNumber = 8 thisUpdate = 19:00 nextUpdate = 20:00 BaseCRLNumber = 7 CertificateList = {67k}

· 취소 사유
  a : 직장변경
  k : 키 손상
  h : 인증서 효력정지
  r : 효력 정지된 인증서 취소 목록을 CRL로부터 제거함(복구)

취소 사유와 부호는 인증기관 정책에 따라 변경될 수 있음.

1) 전형적인 Delta-CRL 발급 방법

Full-CRL은 3시간마다 한번씩 발행하고 Delta-CRL은 시간마다 한번씩 발행한다. 발행의 편이를 위하여, 발행자는 첫 번째 Full-CRL을 발행함과 동시에 Delta-CRL을 발행하기 시작하고 Delta-CRL은 항상 이전에 발행된 Full-CRL을 기반으로 사용할 수 있다. Delta-CRL 번호 4로부터 시작하여, Full-CRL과 동시에 발행되는 Delta-CRL은 Base-CRL로 이전에 발행되었던 Full-CRL을 사용한다. 그러나 Delta-CRL들은 3시간 이상의 이력을 제공하지 않는다.

▶ 표 2에 발행된 Delta-CRL 관련 사건 일지

- 인증서 14는 첫 CRL이 발행된 12:00 이전에 키 손상으로 취소되었다.
- 인증서 124는 12:00 에서 13:00 사이에서 키 손상으로 취소되었다.
- 인증서 39는 14:00 에서 15:00 사이에 효력이 유보되었다. 그리고 이 유보는 16:00와 17:00 사이에 취소되었다.
- 인증서 67은 15:00에서 16:00사이에 직장 변경으로 취소되었다. 인증서 67의 취소 사유는 18:00에서 19:00 사이에 키 손상으로 변경되었다.

2) 슬라이딩 윈도우 방식을 이용한 Delta-CRL 발급방법

아래의 예는 Delta-CRL을 발행하는 "슬라이딩 윈도우" 방법을 나타낸다.

이 방법에서, Full-CRL들은 3시간마다 한번씩 발행되고, 델타는 매 한시간마다 한번씩 발행된다. 발행자는 full-CRL과 동시에 Delta-CRL 발행을 개시한다고 가정한다. cRLNumber 7부터 시작하여, full CRL과 동시에 발행된 Delta-CRL은 Base-CRL로서 이전에 발행된 full CRL을 이용하지 않고 대신에 이전 CRL을 이용한다. 이 Delta-CRL들은 6시간 이상의 이력을 제공하지 않는다.[10]

▶ 표 3에 발행된 Delta-CRL 관련 사건 일지

- 인증서 14는 첫 CRL이 발행된 12:00 이전에 키 손상으로 취소되었다.
- 인증서 124는 12:00 13:00 사이에서 키 손상으로 취소되었다.
- 인증서 39는 14:00 에서 15:00 사이에 효력이 유보되었다. 그리고 이 유보는 16:00와 17:00 사이에 취소되었다.
- 인증서 67은 15:00에서 16:00사이에 직장 변경으로 취소되었다. 인증서 67의 취소 사유는 18:00에서 19:00 사이에 키 손상으로 변경되었다.

3) 복사/전달 지연 시간을 고려한 Delta-CRL 발급방법

이 방법에서, full-CRL과 Delta-CRL은 저장소 시스템 도처에 복사될 것이다. 데이터는 파일의 크기에 따라서 다른 속도로 시스템 도처에 복사될 것이다. CA 관리자는 full-CRL이 3시간 이내에 시스템 전반에 유용하다고 추정한다. Delta-CRL은 15분 이내에 유용하다. (초기 CRL 은 작고, Delta-CRL 같이 전파될 것이다.)[10]

이 방법은 Delta-CRL을 발행하는 "슬라이딩 윈도우" 방법을 사용한다. 그러나 전파를 고려하여 thisUpdate 와 nextUpdate 시간을 중복되도록 한다. 이 예제에서, full-CRL 은 매 3시간마다 한번씩 발행되고, Delta-CRL은 매 45분마다 한번씩 발행된다. 일관성을 위하여 발행자는 full-CRL 과 동시에 delta-CRL의 발행을 시작한다. cRLNumber 7로 시작하여, full CRL과 동시에 발행된 Delta-CRL은 기반으로 직전에 발행된 full CRL을 이용하는 대신에 이전 CRL을 이용한다. 이 Delta-CRL은 6시간 이상의 이력은 제공하지 않는다.

▶ 표 4에 발행된 Delta-CRL 관련 사건 일지

- 인증서 14는 첫 CRL이 발행된 12:00 이전에 키 손상으로 취소되었다.
- 인증서 124는 12:00 에서 13:00 사이에 키 손상으로 취소되었다.
- 인증서 39는 14:00 에서 15:00 사이에 효력이 유보되었다. 그리고 이 유보는 16:00와 17:00 사이에 취소되었다.

표 3 슬라이딩 윈도우 방식을 이용한 Delta-CRL 발급방법

current time	Revoked certificates	Full CRL	Delta-CRL
12:00	{14k}	cRLNumber = 1 thisUpdate = 12:00 nextUpdate = 15:00 CertificateList = {14k}	cRLNumber = 1 thisUpdate = 12:00 nextUpdate = 13:00 BaseCRLNumber = 1 CertificateList = {}
13:00	{14k, 124k}		cRLNumber = 2 thisUpdate = 13:00 nextUpdate = 14:00 BaseCRLNumber = 1 CertificateList = {124k}
14:00	{14k, 124k}		cRLNumber = 3 thisUpdate = 14:00 nextUpdate = 15:00 BaseCRLNumber = 1 CertificateList = {124k}
15:00	{14k, 124k, 39h}	cRLNumber = 4 thisUpdate = 15:00 nextUpdate = 18:00 CertificateList = {14k, 124k, 39h}	cRLNumber = 4 thisUpdate = 15:00 nextUpdate = 16:00 BaseCRLNumber = 1 CertificateList = {124k, 39h}
16:00	{14k, 124k, 39h, 67a}		cRLNumber = 5 thisUpdate = 16:00 nextUpdate = 17:00 BaseCRLNumber = 1 CertificateList = {124k, 39h, 67a}
17:00	{14k, 124k, 67a}		cRLNumber = 6 thisUpdate = 17:00 nextUpdate = 18:00 BaseCRLNumber = 1 CertificateList = {124k, 39r, 67a}
18:00	{14k, 124k, 67a}	cRLNumber = 7 thisUpdate = 18:00 nextUpdate = 21:00 CertificateList = {14k, 124k, 67a}	cRLNumber = 7 thisUpdate = 18:00 nextUpdate = 19:00 BaseCRLNumber = 1 CertificateList = {124k, 39r, 67a}
19:00	{14k, 124k, 67k}		cRLNumber = 8 thisUpdate = 19:00 nextUpdate = 20:00 BaseCRLNumber = 4 CertificateList = {39r, 67k}

표 4 복사/전달 지연 시간을 고려한 Delta-CRL 발급방법

Current time	Revoked certificates	Full CRL	Delta-CRL
12:00	{14k}	cRLNumber = 1 thisUpdate = 12:00 nextUpdate = 18:00 CertificateList = {14k}	cRLNumber = 1 thisUpdate = 12:00 nextUpdate = 13:00 BaseCRLNumber = 1 CertificateList = {}
12:45	{14k, 124k}		cRLNumber = 2 thisUpdate = 12:45 nextUpdate = 13:45 BaseCRLNumber = 1 CertificateList = {124k}
13:30	{14k, 124k}		cRLNumber = 3 thisUpdate = 13:30 nextUpdate = 14:30 BaseCRLNumber = 1 CertificateList = {124k}
14:15	{14k, 124k}		cRLNumber = 4 thisUpdate = 14:15 nextUpdate = 15:15 BaseCRLNumber = 1 CertificateList = {124k}
15:00	{14k, 124k, 39h}	cRLNumber = 5 thisUpdate = 15:00 nextUpdate = 21:00 CertificateList = {14k, 124k, 339h}	cRLNumber = 5 thisUpdate = 15:00 nextUpdate = 16:00 BaseCRLNumber = 1 CertificateList = {124k, 39h}
15:45	{14k, 124k, 39h, 667a}		cRLNumber = 6 thisUpdate = 15:45 nextUpdate = 16:45 BaseCRLNumber = 1 CertificateList = {124k, 39h, 67a}
16:30	{14k, 124k, 67a}		cRLNumber = 7 thisUpdate = 16:30 nextUpdate = 17:30 BaseCRLNumber = 1 CertificateList = {124k, 39r, 67a}
17:15	{14k, 124k, 67a}		cRLNumber = 8 thisUpdate = 17:15 nextUpdate = 18:15 BaseCRLNumber = 1 CertificateList = {124k, 339r, 67a}
18:00	{14k, 124k, 67a}	cRLNumber = 9 thisUpdate = 18:00 nextUpdate = 24:00 CertificateList = {14k, 124k, 67a}	cRLNumber = 9 thisUpdate = 18:00 nextUpdate = 19:00 BaseCRLNumber = 5 CertificateList = {124k, 39r, 67a}
18:45	{14k, 124k, 67k}		cRLNumber = 10 thisUpdate = 18:45 nextUpdate = 19:45 BaseCRLNumber = 5 CertificateList = {39r, 67k}

- 인증서 67은 15:00에서 16:00사이에 직장 변경으로 취소되었다. 인증서 67의 취소 사유는 18:00에서 19:00 사이에 키 손상으로 변경되었다.

V. 결론

본 논문에서는 Base-CRL과 Delta-CRL의 각각의 필드들을 분석하였고, 주기적으로 발급하는 Delta-CRL의 발급 방법과 슬라이딩 윈도우 방식을 채택하여 Full-CRL과 Delta-CRL을 발급하는 방법, 또 복사/전달 지연 시간을 고려한 Delta-CRL 발급 방법을 분석하였다. 그리고 DistributionPoint 확장자의 reasons 필드를 이용하여 Scope 별로 CRL을 발행하는 방안을 제안하였다.

제안된 시스템의 목적은 Delta-CRL을 발급함으로써 분산된 네트워크의 부하를 줄이고 데이터베이스의 저장 능력을 늘리는 것에 있다. 그리고 Scope별로 CRL을 발행함으로써 CRL을 저장하는 저장소나 데이터베이스의 부하를 줄일 수 있는 장점이 있다.

또한 본 논문에서는 국내 KISA와 공인인증기관을 위한 인증서 취소목록인 CARL과 CRL 발급 및 Delta-CRL 발급에 대한 정책을 논의하였고 그에 대한 발급주기와 Scope, 그리고 Delta-CRL의 발급 범위를 제시하였다.

현재 미국 연방 정부 브리지 인증기관 인증서 정책에서는 키 손상과 reasons 필드가 생략된, 즉 전체적인 취소사유를 포함하는 두 가지의 Scope으로 Delta-CRL을 발급하는 시스템이 주로 쓰이고 있으며 본 논문에서 또한 두 가지 Scope으로 Delta-CRL을 발급하는 시스템을 정책으로 제시하고 있다.

참고문헌

[1] David A. Cooper, "A More Efficient Use of Delta-CRLs", Proceeding of 2000 IEEE Symposium on Security and Privacy, 2000

[2] IETF homepage, http://www.ietf.org/, 1999.

[3] C. Adams, S. Farrell, Certificate Management Protocols, http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki3cmp-08.txt, 1998. 5

[4] David A. Cooper, "A Model of Certificate Revocation", Proceeding of Fifteenth Annual Computer Security Applications Conference, 12, 1999.

[5] 정보보호센터 홈페이지 연구자료들, http://www.kisa.or.kr/, 1999.

[6] Public-Key Infrastructure (X.509) (pkix), http://www.ietf.org/html.charters/pkix-charter.html, 1998. 4

[7] IETF, Security Area, "X.509 (pkix) Document", http://www.ietf.org, 1999,7.

[8] ITU and ISO/IEC Final Proposed Draft Amendment on Certificate Extensions April 1999

[9] R. Housley, W. Ford, W. Polk, D. Solo "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", http://www.ietf.org/internet-drafts/draft-ietf-pkix-new-part1-08.txt, 7, 2001.

[10] IETF Internal Document, IETF Society, 2001